

日 本 国 特 許 庁
JAPAN PATENT OFFICE

24.07.03

REC'D 12 SEP 2003

WIPO PCT

10/522176

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年 7月25日

出 願 番 号
Application Number: 特願2002-216750
[ST. 10/C]: [JP2002-216750]

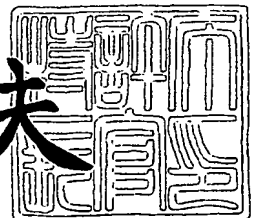
出 願 人
Applicant(s): 三洋電機株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 8月28日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 1020333

【提出日】 平成14年 7月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 11/08

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社
社内

【氏名】 堀 吉宏

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社
会社 所沢工場内

【氏名】 多田 謙一郎

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日
立製作所 システム開発研究所内

【氏名】 平井 達哉

【発明者】

【住所又は居所】 東京都千代田区丸の内1-3-1 東京銀行協会ビル1
4F フェニックステクノロジーズ株式会社内

【氏名】 津留 雅文

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 長谷部 高行

【特許出願人】

【識別番号】 000001889

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号

【氏名又は名称】 三洋電機株式会社

【特許出願人】

【識別番号】 000005016
【住所又は居所】 東京都目黒区目黒 1 丁目 4 番 1 号
【氏名又は名称】 パイオニア株式会社

【特許出願人】

【識別番号】 000005108
【住所又は居所】 東京都千代田区神田駿河台 4 丁目 6 番地
【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 300017636
【住所又は居所】 東京都千代田区丸の内 1-3-1 東京銀行協会ビル 14 F
【氏名又は名称】 フェニックステクノロジーズ株式会社

【特許出願人】

【識別番号】 000005223
【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100083703
【弁理士】
【氏名又は名称】 仲村 義平

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【選任した代理人】

【識別番号】 100098316

【弁理士】

【氏名又は名称】 野田 久登

【選任した代理人】

【識別番号】 100109162

【弁理士】

【氏名又は名称】 酒井 將行

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006995

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ記憶装置

【特許請求の範囲】

【請求項 1】 一定の手順に従って機密データの入出力を行ない、前記機密データを記憶し、かつ、前記一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置であって、

外部とデータの入出力を行なうインターフェースと、

複数の前記機密データを格納するデータ記憶部と、

前記機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、

前記機密データの入出力を制御する制御部とを備え、

前記ログ記憶部は、それぞれ 1 つの前記履歴情報を格納する 2 つ以上の領域を循環的に利用するリングバッファとして設けられており、

前記ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、

前記制御部は、前記機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報を前記インターフェースを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に前記受取った識別情報を含む前記機密データの入出力処理に対する履歴情報を新たに格納する、データ記憶装置。

【請求項 2】 履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報を前記インタフェースを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、前記最新領域に格納されている履歴情報の一部または全てを前記インタフェースを介して出力する、請求項 1 に記載のデータ記憶装置。

【請求項 3】 履歴情報の出力を伴う前記機密データの入力処理において、前記制御部は、入出力の対象となる機密データの識別情報を前記インタフェー

スを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの入力処理に対する新たな履歴情報として格納し、前記特定された最古領域に格納された履歴情報の一部または全てを前記インタフェースを介して出力する、請求項 1 に記載のデータ記憶装置。

【請求項 4】 他の装置によって前記一定の手順の進行によって記録されたもう 1 つの履歴情報の入力を伴う前記機密データの再出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報および前記もう 1 つの履歴情報とを前記インタフェースを介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納された履歴情報と、前記受取ったもう 1 つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求項 2 または請求項 3 に記載のデータ記憶装置。

【請求項 5】 他の装置によって前記一定の手順の進行に従って記録されたもう 1 つの履歴情報の入力を伴う前記機密データの出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報および前記もう 1 つの履歴情報を前記インタフェースを介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの出力処理に対する新たな履歴情報として格納し、前記特定した最古領域に格納された履歴情報と、前記受取ったもう 1 つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求項 2 または請求項 3 に記載のデータ記憶装置。

【請求項 6】 前記最古領域を特定した後、

前記制御部は、前記入出力処理における一定の手順が終了あるいは中止されるまでの間、前記特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する、請求項 1 から請求項 5 のいずれか 1 項に記載のデータ記憶装置。

【請求項 7】 前記複数の履歴情報の各々は、前記ログ記憶部へ記憶された

順序を識別するための管理番号をさらに含み、

前記管理番号は、前記ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される前記最古領域を検出する、請求項1から請求項6のいずれか1項に記載のデータ記憶装置。

【請求項8】 前記ログ記憶部は、 N (N は2以上の自然数) 個の領域を循環的に利用するリングバッファからなり、

前記管理番号は、 M (M は、 $N < M$ を満たす自然数) の剰余系からなる、請求項7に記載のデータ記憶装置。

【請求項9】 前記制御部は、前記ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号を取得し、その取得した2つの管理番号の差に基づいて、2つの当該管理番号を含む2つの履歴情報が連続して格納されたか否かを判定し、2つの履歴情報が不連続に格納された履歴情報であるとき、前記連続する2つの領域のうち、後続領域を前記最古領域として検出する、請求項8に記載のデータ記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶するデータ記憶装置に関し、特に、マルチアクセスが可能なデータ記憶装置においてコピーされた情報に対する著作権保護を可能とするデータ記憶装置に関するものである。

【0002】

【従来の技術】

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができなないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】

しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0007】

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0008】

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカー

ドの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセンスを識別するためのライセンスID、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築し、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

【0009】

メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。最終的に、携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

【0010】

また、メモリカードは、他のメモリカードとの間でライセンスの移動または複製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

【0011】

さらに、送受信中の不慮の中断によってライセンスが消失した場合に、その処理を再開でき、かつ、ライセンスの重複送信を防ぐためにライセンスの入出力に

関する直近の履歴情報を記録し、必要に応じて出力する機能をメモリカードは備えている。送信元である配信サーバあるいはメモリカードは、送信先のメモリカードから履歴情報を取得して、この履歴情報に従ってライセンスの送受信の再開を判断する。履歴情報は、ライセンスIDと送受信を示すステータス情報を含んでいる。

【0012】

このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。また、著作権者の権利を保護することができる。

【0013】

【発明が解決しようとする課題】

しかし、従来のメモリカードにおいては、直近の履歴情報を保持するのみで、中断後、他のライセンスに対する送受信を行った場合に先の中断に対する履歴情報が消えてしまう。このような場合、複数の履歴情報を格納することにより、ユーザの利便性を改善することが可能である。

【0014】

また、記憶素子に対するアクセスの高速化や、記憶素子の大容量化に伴い、複数のライセンスの送受信を並行して行なう要求が発生することが、今後、予想される。その場合、少なくとも並行して行われる処理に関する履歴情報を格納できるようにする必要性が生ずる。

【0015】

このように、複数の履歴情報を格納できるようにする場合に、ライセンスの受信後に、該ライセンスを他のメモリカードに対して移したとすると、同一のライセンスIDに対して異なったステータスを持つ履歴情報が格納されるという問題が生じる。

【0016】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開

可能とするための履歴情報を重複することなく複数格納できるデータ記憶装置を提供することである。

【0017】

【課題を解決するための手段】

この発明によれば、データ記憶装置は、一定の手順に従って機密データの入出力を行ない、機密データを記憶し、かつ、一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置であって、外部とデータの入出力を行なうインターフェースと、複数の機密データを格納するデータ記憶部と、機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、機密データの入出力を制御する制御部とを備え、ログ記憶部は、それぞれ1つの履歴情報を格納する2つ以上の領域を循環的に利用するリングバッファとして設けられており、ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、制御部は、機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に受取った識別情報を含む機密データの入出力処理に対する履歴情報を新たに格納する。

【0018】

好ましくは、履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、最新領域に格納されている履歴情報の一部または全てをインタフェースを介して出力する。

【0019】

好ましくは、履歴情報の出力を伴う前記機密データの入力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識

別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの入力処理に対する新たな履歴情報として格納し、特定された最古領域に格納された履歴情報の一部または全てをインタフェースを介して出力する。

【0020】

好ましくは、他の装置によって一定の手順の進行によって記録されたもう1つの履歴情報の入力を伴う機密データの再出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報とをインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

【0021】

好ましくは、他の装置によって一定の手順の進行に従って記録されたもう1つの履歴情報の入力を伴う機密データの出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう1つの履歴情報をインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの出力処理に対する新たな履歴情報として格納し、特定した最古領域に格納された履歴情報と、受取ったもう1つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

【0022】

好ましくは、最古領域を特定した後、制御部は、入出力処理における一定の手順が終了あるいは中止されるまでの間、特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する。

【0023】

好ましくは、複数の履歴情報の各々は、ログ記憶部へ記憶された順序を識別するための管理番号をさらに含み、管理番号は、ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号に基づいて、

古い履歴情報が格納される最古領域を検出する。

【0024】

好ましくは、ログ記憶部は、 N (N は2以上の自然数) 個の領域を循環的に利用するリングバッファからなり、管理番号は、 M (M は、 $N < M$ を満たす自然数) の剰余系からなる。

【0025】

好ましくは、制御部は、ログ記憶部に連続して配置された2つの領域に格納された2つの履歴情報に含まれる各々の管理番号を取得し、その取得した2つの管理番号の差に基づいて、2つの当該管理番号を含む2つの履歴情報が連続して格納されたか否かを判定し、2つの履歴情報が不連続に格納された履歴情報であるとき、連続する2つの領域のうち、後続領域を最古領域として検出する。

【0026】

したがって、この発明によれば、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための複数の履歴情報を重複することなく格納できる。

【0027】

【発明の実施の形態】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0028】

〔実施の形態1〕

図1は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0029】

なお、以下では、デジタル放送網により配信された映像データを端末装置10により受信して端末装置10に装着されたデータ記憶装置であるHD（ハードディスクドライブ）20に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク30に端末装置10と接続されるライセン

ス提供装置 40 からネットワーク 30 を介してから受信して HD 20 に格納し、暗号化された映像データを端末装置 10 に内蔵された専用の再生回路（図示せず）にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモリカードなどにおいても適用することが可能である。

【0030】

図 1 を参照して、端末装置 10 は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ 11 を介して受信し、HD 20 に記憶する。暗号化されたコンテンツデータ（以下、暗号化コンテンツデータとも呼ぶ）を復号するためのコンテンツ鍵を含むライセンスを管理し、かつ、配信するライセンス提供装置 40 は、ライセンスの配信を求めてアクセスしてきた端末装置 10 に装着された HD 20 が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、HD 20 が正当なデータ記憶装置であった場合のみ、端末装置 10 に対して HD 20 においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置 10 は、ネットワーク 30 に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着された HD 20 へ送信する。

【0031】

図 1 においては、たとえば、HD 20 は、端末装置 10 に着脱可能な構成となっている。端末装置 10 に装着された HD 20 は、端末装置 10 により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえで HD 20 内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置 10 に与える。

【0032】

そして、端末装置10のユーザは、端末装置10においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

【0033】

このような構成とすることで、端末装置10のユーザは、ライセンス管理機能を備えた正規の認証データを有するHD20を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

【0034】

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、ライセンスを管理するライセンス提供装置40であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置40とは別の配信サーバであってもよい。また、他のユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

【0035】

したがって、本発明の実施の形態においては、HD20、端末装置10およびライセンス提供装置40のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したときに、ライセンスが重複して存在することがないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

【0036】

図2は、図1に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

【0037】

データD_cは、コンテンツデータであって、ここでは映像データである。データD_cは、コンテンツ鍵K_cで復号可能な暗号化が施される。コンテンツ鍵K_cによって復号可能な暗号化が施された暗号化コンテンツデータE (K_c, D_c) が、この形式でデジタル放送網により端末装置10のユーザに配布される。

【0038】

なお、以下においては、E (X, Y) という表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。また、データD_cに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報D_iが配布される。

【0039】

また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスID (LID) が端末装置10を介してライセンス提供装置40とHD20との間でやり取りされる。さらに、ライセンスとしては、データD_cおよびコンテンツ鍵K_cを識別するためのコードであるデータID (DID) や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ACが存在する。

【0040】

コンテンツ鍵K_cと、制御情報ACと、DIDと、LIDとを併せて、以後、ライセンスLICと総称することとする。DIDは、データD_cとコンテンツ鍵K_cとの対に対して割り当てられた識別情報、すなわち、暗号化データE (K_c, D_c) を識別するための識別情報となる。DIDは、ライセンスLICの他に、暗号化データE (K_c, D_c) とともに常に扱われる付加情報D_iにも含まれ、参照できるようになっている。

【0041】

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0042】

HD 20などのデータ記憶装置および端末装置10などに備えられる再生回路には、固有のクラス公開鍵 $KP_{cm y}$ および $KP_{cp y}$ がそれぞれ設けられ、クラス公開鍵 $KP_{cm y}$ および $KP_{cp y}$ は、データ記憶装置に固有のクラス秘密鍵 $K_{cm y}$ および再生回路に固有のクラス秘密鍵 $K_{cp y}$ によってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「y」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0043】

また、データ記憶装置のクラス証明書として $C_{m y}$ が設けられ、再生回路のクラス証明書として $C_{p y}$ が設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。

【0044】

データ記憶装置のクラス証明書 $C_{m y}$ は、 $KP_{cm y} // I_{cm y} // E(K_a, H(KP_{cm y} // I_{cm y}))$ の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書 $C_{p y}$ は、 $KP_{cp y} // I_{cp y} // E(K_a, H(KP_{cp y} // I_{cp y}))$ の形式で出荷時に再生回路に記憶される。ここで、 $X // Y$ は、XとYとの連結を表わし、 $H(X)$ は、ハッシュ関数により演算されたデータXのハッシュ値を表わす。マスタ鍵 K_a は、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報 $I_{cm y}$ 、 $I_{cp y}$ は、クラスごとの機器に関する情報およびクラス公開鍵を含む情報データである。

【0045】

また、 $E(K_a, H(KP_{cm y} // I_{cm y}))$ および $E(K_a, H(KP_{cp y} // I_{cp y}))$ は、それぞれ $KP_{cm y} // I_{cm y}$ および $KP_{cp y} // I_{cp y}$ に対する電子署名を行なった署名データである。

【0046】

なお、認証局は、署名データを作成する公的な第三者機関であり、署名データ $E(K_a, H(KP_{cm_y} // I_{cm_y}))$ および $E(K_a, H(KP_{cp_y} // I_{cp_y}))$ は、認証局によって生成される。

【0047】

さらに、データ記憶装置に対して安全かつ確実にライセンスLICを送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵 KP_{om_z} と、個別公開鍵 KP_{om_z} で暗号化されたデータを復号することが可能な個別秘密鍵 K_{om_z} とが存在する。ここで、記号「z」は、データ記憶装置を個別に識別するための識別子である。

【0048】

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置40、データ記憶装置(HD20)、および端末装置10の再生回路において生成されるセッション鍵 K_{s1_x} 、 K_{s2_x} が用いられる。

【0049】

ここで、セッション鍵 K_{s1_x} 、 K_{s2_x} は、ライセンス提供装置40、データ記憶装置(HD20)、もしくは端末装置10の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。

「セッション」には、ライセンス提供装置40からデータ記憶装置(HD20)へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置(HD20)から端末装置10の再生回路へライセンスを出力する「再生許諾セッション」がある。

【0050】

これらのセッション鍵 K_{s1_x} 、 K_{s2_x} は、各セッションごとに固有の値を有することにより、ライセンス提供装置40、データ記憶装置(HD20)、および端末装置10の再生回路によって管理される。具体的には、セッション鍵 K_{s1_x} は、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵 K_{s2_x} は、ライセンスの受信側によってセッションごとに発生される。なお、記号「x」は、セッションにおける一連の処理

を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスLIC、またはコンテンツ鍵を含むライセンスLICの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0051】

図4は、図1に示したライセンス提供装置40の構成を示す概略ブロック図である。

【0052】

ライセンス提供装置40は、管理対象のライセンスを保持するデータベースであるコンテンツDB402と、ライセンスを配信する配信セッションにおける全ての通信記録を随時記憶し、保持するデータベースであるログDB404と、コンテンツDB402およびログDB404とバスBS1を介してデータをやり取りし、所定の処理を行なうためのデータ処理部410と、ネットワーク30を介して端末装置10とデータ処理部410との間でデータ授受を行なうための通信装置450とを備える。

【0053】

データ処理部410は、バスBS1上のデータに応じて、データ処理部410の動作を制御するための配信制御部412と、配信制御部412により制御されて、配信セッション時にセッション鍵 K_{s1x} を発生するためのセッション鍵発生部414と、端末装置10から送られてくるHD20のクラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ を復号するためのHD20の認証鍵 KPa を保持する KPa 保持部416と、HD20から送られてきたクラス証明書 C_{my} を通信装置450およびバスBS1を介して受け、 KPa 保持部416から受ける認証鍵 KPa によって復号処理を行ない、クラス証明書 C_{my} に含まれる署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ の復号処理と、クラス証明書 C_{my} に含まれる $KP_{cmy} // I_{cmy}$ のハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書 C_{my} の検証を行なう認証部418と、配信セッションごとに、セッション鍵発生部414に

より生成されたセッション鍵 K_{s1x} を認証部 418 によってクラス証明書 C_{my} から抽出したクラス公開鍵 $K_{P_{cm_y}}$ を用いて暗号化し、バス $BS1$ に出力するための暗号処理部 420 と、セッション鍵 K_{s1x} によって暗号化された上で送信されたデータをバス $BS1$ より受け、復号処理を行なう復号処理部 422 とを含む。

【0054】

データ処理部 410 は、さらに、配信制御部 412 から与えられるライセンス LIC を、復号処理部 422 によって得られたデータ記憶装置ごとに固有な個別公開鍵 $K_{P_{omz}}$ によって暗号化するための暗号処理部 424 と、暗号処理部 424 の出力を、復号処理部 422 から与えられるセッション鍵 K_{s2x} によってさらに暗号化してバス $BS1$ に出力するための暗号処理部 426 とを含む。

【0055】

なお、個別公開鍵 $K_{P_{omz}}$ およびセッション鍵 K_{s2x} は、セッション鍵 K_{s1x} によって暗号化されたうえで端末装置 10 から提供される。復号処理部 422 は、これを復号して個別公開鍵 $K_{P_{omz}}$ を得る。

【0056】

ライセンス提供装置 40 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0057】

図 5 は、図 1 に示した端末装置 10 の構成を説明するための概略ブロック図である。

【0058】

端末装置 10 は、デジタル放送網によって伝送される信号を受信するアンテナ 102 と、アンテナ 102 からの信号を復調してデータに変換、あるいはアンテナ 102 から送信するデータを変調してアンテナ 102 に与える受信部 104 と、端末装置 10 をネットワーク 30 に接続するモデム 106 と、端末装置 10 の各部のデータ授受を行なうバス $BS2$ と、バス $BS2$ を介して端末装置 10 の動作を制御するコントローラ 108 と、HD 20 とバス $BS2$ との間のデータの授受を制御する HD インターフェース部 110 とを含む。

【0059】

端末装置10は、さらに、上述したクラス証明書Cp_yを保持する認証データ保持部1502を含む。ここで、端末装置10のクラスを識別する識別子yは、 $y=3$ であるとする。

【0060】

端末装置10は、さらに、クラス固有の復号鍵であるクラス秘密鍵Kcp₃を保持するKcp保持部1504と、バスBS2から受けたデータをクラス秘密鍵Kcp₃によって復号し、HD20によって発生されたセッション鍵Ks_{1x}を得る復号処理部1506とを含む。

【0061】

端末装置10は、さらに、HD20に記憶されたコンテンツデータの再生を行なう再生許諾セッションにおいて、HD20との間でやり取りされるデータを暗号化するためのセッション鍵Ks_{2x}を乱数等により発生するセッション鍵発生部1508と、HD20からコンテンツ鍵Kcを受取る際に、セッション鍵発生部1508により発生されたセッション鍵Ks_{2x}を復号処理部1506によって得られたセッション鍵Ks_{1x}によって暗号化し、バスBS2に出力する暗号処理部1510と、バスBS2上のデータをセッション鍵Ks_{2x}によって復号して、コンテンツ鍵Kcを出力する復号処理部1512と、バスBS2より暗号化コンテンツデータE(Kc, Dc)を受けて、復号処理部1512からのコンテンツ鍵Kcによって暗号化コンテンツデータE(Kc, Dc)を復号してデータDcを再生部1516へ出力する復号処理部1514と、復号処理部1514からの出力を受けてコンテンツを再生するための再生部1516と、再生部1516の出力をデジタル信号からアナログ信号に変換するDA変換部1518と、DA変換部1518の出力をテレビモニターなどの外部出力装置(図示省略)へ出力するための端子1520とを含む。

【0062】

なお、図5においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路150を構成する。再生回路150は、セキュリティを向上させるために1チップ構成の半導体デバイスである

ことが好ましい。さらには、再生回路150は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

【0063】

端末装置10の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0064】

ここでは、端末装置10は、暗号化コンテンツデータを受信する機能、ライセンスの配信を受ける機能、再生許諾によって暗号化コンテンツデータを再生する機能を備えていたが、HD20が端末装置10から脱着可能なデータ記憶装置であることから明らかなように、これらの機能を別々の装置によって実現してもよい。この場合、目的とする機能を実現する装置にHD20を装着することで容易に実現できる。

【0065】

図6は、図1に示すHD20の構成を説明するための概略ブロック図である。

すでに説明したように、データ記憶装置であるHD20には、クラス公開鍵 K_{Pcm} とクラス秘密鍵 K_{cm} のペア、および個別公開鍵 K_{Pom} と個別秘密鍵 K_{om} のペアが設けられるが、HD20においては、これらを識別する識別子 $y=1$ 、識別子 $z=2$ で表されるものとする。

【0066】

したがって、HD20は、クラス証明書 C_{m1} として認証データ $K_{Pcm1}/I_{cm1}/E(K_a, H(K_{Pcm1}/I_{cm1}))$ を保持する認証データ保持部202と、クラス秘密鍵 K_{cm1} を保持する K_{cm} 保持部204と、個別秘密鍵 K_{om2} を保持する K_{om} 保持部206と、個別秘密鍵 K_{om2} によって復号可能な個別公開鍵 K_{Pom2} を保持する K_{Pom} 保持部208とを含む。

【0067】

このように、データ記憶装置（ここではHD20）の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をデータ記憶装置単位で実行することが可能になる。

【0068】

HD 20は、さらに、端末装置10のHDインターフェース部110と端子210を介して信号を授受するATA (A T - A t t a c h m e n t) インターフェース部212と、HD 20におけるデータ伝送路であるバスBS 3と、ATAインターフェース部212からコントローラ214を介してバスBS 3に出力されたデータを、Kom保持部206により与えられた個別秘密鍵Kom 2により復号し、ライセンス提供装置40から配信されたライセンスLICをセキュアデータ記憶部250へ出力する復号処理部216と、KPa保持部218から認証鍵KPaを受け、バスBS 3に出力されたデータの認証鍵KPaによる復号処理を実行して復号結果をコントローラ214へ出力し、かつ、得られたクラス公開鍵K P c m 1を暗号処理部222へ出力する認証部220と、切換スイッチ260によって選択的に与えられるセッション鍵K s 1 xまたはK s 2 xによって、切換スイッチ262によって選択的に与えられるデータを暗号化してバスBS 3に出力する暗号処理部224とを含む。

【0069】

HD 20は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵K s 1 x, K s 2 xを発生するセッション鍵発生部226と、セッション鍵発生部226の出力したセッション鍵K s 1 xを認証部220によって得られる端末装置10の再生回路150のクラス公開鍵K P c p yあるいは他のデータ記憶装置 (HD 21とする) のクラス公開鍵K P c m yによって暗号化してバスBS 3に送出する暗号処理部222と、バスBS 3よりセッション鍵K s 2 xによって暗号化されたデータを受けてセッション鍵発生部226より得たセッション鍵K s 1 xまたはK s 2 xによって復号する復号処理部228とを含む。

【0070】

HD 20は、さらに、バスBS 3上のデータをクラス公開鍵K P c m 1と対をなすクラス秘密鍵K c m 1によって復号するための復号処理部230と、ライセンスLICをHD 20からHD 21へ移動または複製するために出力する際に、提供先のHD 21から受信した個別公開鍵K P o m z (z ≠ 2) によりライセンスLICを暗号化する暗号処理部232とを含む。

【0071】

HD20は、さらに、暗号化コンテンツデータE (K_c , D_c) を再生するためのライセンスLICと、HD20が処理しているセッションの処理記録であるログとをバスBS3より受けて記憶するセキュアデータ記憶部250を含む。そして、ライセンスLICは、セキュアデータ記憶部250内のセキュアデータ記憶部250に格納され、ログは、セキュアデータ記憶部250内のログメモリ253に格納される。セキュアデータ記憶部250は、たとえば半導体メモリによって構成される。

【0072】

図7は、セキュアデータ記憶部250におけるメモリ構成を示した図である。

図7を参照して、セキュアデータ記憶部250は、ライセンス領域251と、有効フラグ領域252と、ログメモリ253とを含む。

【0073】

ライセンス領域251は、L個 (Lは自然数) の領域2511～251Lから成り、それぞれ1つのライセンス (コンテンツ鍵 K_c 、制御情報AC、ライセンスID (LID)、データID (DID)) を格納する。

【0074】

領域2511～251Lに格納された複数のライセンスの各々は、アドレス (以下、LBA: Logical Block Addressと称する。) によって管理される。そして、各セッションにおいて記憶あるいは読出されるライセンスLICは、全てLBAにより特定される。

【0075】

領域2511～251Lに対応して $\max LBA + 1 \sim \max LBA + L$ のLBAが付与されているものとする。たとえば、領域2513に格納されたライセンスLICは、LBA: $\max LBA + 3$ によって特定される。このとき、LBA: $0 \sim \max LBA$ は、ノーマルデータ記憶領域270に割当てられるものとする。詳細は後述する。

【0076】

なお、ライセンス領域251には、ノーマルデータ記憶領域270に割当てら

れたLBA (0～max LBA) に続く値、すなわち、max LBA+1～max LBA+LがLBAとして割当てられると説明したが、ライセンス領域251に割当てたLBAを限定するものではない。ライセンス領域251に割当てたL個のLBAによって、それぞれが領域2511～251Lのいずれか1つを指定できる値であればいかなる値であってもよく、ノーマルデータ記憶領域270に割当てたLBAと重複する値、あるいは、独立した値をLBAとして割当ててもよい。

【0077】

また、有効フラグ領域252は、セキュアデータ記憶部250上の記憶位置を特定するLBAそれぞれに対応して設けられ、対応するLBAによって特定される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

【0078】

有効フラグ領域252は、領域2521～252Lから成り、領域2521～252Lは、それぞれ、対応する領域2511～251Lに格納されたライセンスLICの”有効”、または”無効”を格納する。

【0079】

有効フラグ領域252のフラグが”有効”であるとき、フラグに対応するLBAによって特定されるセキュアデータ記憶部250上の記憶位置に記憶されているライセンスLICは利用可能であり、ユーザはそのライセンスLIC内のコンテンツ鍵Kcを再生許諾によって読出して、対応する暗号化コンテンツデータを復号し、コンテンツデータを再生したり、そのライセンスLICを他のデータ記憶装置に移動・複製することができる。

【0080】

一方、有効フラグ領域252のフラグが”無効”であるとき、そのフラグに対応するLBAによって特定されるセキュアデータ記憶部250上の記憶位置に記憶されているライセンスLICは利用不可であり、HD20のコントローラ214によって、そのLBAからのライセンスLICは拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンスLICに対応したコンテンツデータを再生することはできない。この有効フラグ領域252の

フラグは、ライセンスの新たな記憶によって”有効”とされ、ライセンスの移動によって”無効”とされる。

【0081】

ログメモリ 253 は、ライセンスを HD 20 に入出力する場合の履歴情報（以下では「ログ」と呼ぶ。）を 1 つ格納する N （ N は自然数）個の領域 2531 ～ 253 N からなるリングメモリである。領域 2531 ～ 253 N は、それぞれ、バンク 0 ～ $N-1$ と称される領域を特定する名称が付与されている。したがって、バンク n （ n は N の剰余系）とは、ログメモリ上の領域 253（ $n-1$ ）を示す。

【0082】

ログメモリ 253 は、複数のログをリング状に格納する。すなわち、ログメモリ 253 は、バンク 0 によって特定される領域 2531 からログの格納を開始し、バンク $N-1$ によって特定される領域 253 N にログを格納すると、再びバンク 0 によって特定される領域 2531 に戻り、ログを格納する。

【0083】

バンク 0 ～ $N-1$ 、すなわち、ログメモリ 253 の領域 2531 ～ 253 N の各々に格納されるログは、管理番号領域 2541 と、ライセンス ID（LID）領域 2542 と、 $Ks2x$ 領域 2543 と、ST1 領域 2544 と、ST2 領域 2545 と、 $KPcmy$ 領域 2546 と、LBA 領域 2547 とを含む。

【0084】

管理番号領域 2541 は、ログをバンク 0 ～ $N-1$ の各々に格納する際に、ログの格納の順序を示す管理番号を格納する。そして、管理番号は、 M （ $M > N$ 、 M は自然数）の剰余系をなして、昇順に付与される。この管理番号を格納することによって、最新のログを格納した、あるいは、最も古いログを格納したバンクを検索することができるようになる。すなわち、最初に管理番号 1 のログがバンク 0 に格納されるとすると、そのログの管理番号領域 2541 は、管理番号”1”を格納する。そして、ライセンスの入出力に伴い、新たなログを格納するごとに、バンク 2 から順に使用し、そのログの管理番号領域 2541 に、新たなログを格納するバンクの直前のバンクに格納される最新のログの管理番号領域 254

1に格納される管理番号に1ずつ増加した管理番号を格納する。したがって、各バンク0～N-1、すなわち、領域2531～253Nに格納されたログの管理番号領域2541から管理番号を読み出せば、管理番号に基づいてそのログが新しいか古いかを判断できる。この判断は、次のようにして行なう。すなわち、連続する2つのバンクn, n+1 (nはNの剰余系) が保持する管理番号が不連続である場合、バンクnには最新のログが、バンクn+1には最も古いログが保持されている。さらに、詳細な説明は、後述する。

【0085】

以降では、特に断らない限り、管理番号に関する表記および演算は全てMの剰余系においてログメモリ253の領域2531～253Nを指定するバンクの番号に関する表記および演算は全てNの剰余系における表記および演算を示している。

【0086】

ライセンスID領域2542は、セッションの対象となるライセンスLICを特定するライセンスID (LID) を格納する。Ks2x領域2543は、セッションにおいてライセンスLICの受信側のデータ記憶装置によって生成されたセッション鍵Ks2xを格納する。

【0087】

ST1領域2544は、動作中のセッションにおける処理の状態を示すステータスST1を格納する。ST2領域2545は、ライセンスID領域2542に格納されるライセンスIDに対応したライセンスの記憶状態を示すステータスST2を格納する。

【0088】

KPcmx領域2546は、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵KPcmxを格納する。LBA領域2547は、各セッションにおいてライセンスLICを読出あるいは記憶するために指示されたLBAを格納する。

【0089】

一連のセッションの処理が進行するにつれて、上記各領域のデータが更新ある

いは参照されていく。ステータス S T 1 は、” 受信待”、” 受信済”、” 送信待” および” 送信済” の 4 状態のいずれかであり、ステータス S T 2 は、” データ有”、” データ無” および” 移動済” の 3 状態のいずれかである。

【0090】

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンス L I C に対して、ログメモリ 253 内のライセンス I D 領域 2541 に格納されているライセンス I D と、L B A 領域 2547 に格納された L B A とによって当該ライセンス L I C の記憶状態が確認され、その確認結果に応じてステータス S T 2 が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ 253 内に格納されているライセンス L I C、セッション鍵 K s 2 x、ステータス S T 1 およびステータス S T 2 を受取って、自身が記録するログの内容と受取ったライセンス L I C、セッション鍵 K s 2 x、ステータス S T 1 およびステータス S T 2 とを確認することにより、再度のライセンスの送信を行なってもよいか否かの判断がされる。

【0091】

なお、セッション鍵 K s 2 x は、各セッションを特定するために記憶され、セッション鍵 K s 2 x を共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

【0092】

また、ステータス S T 2 には、出力ログが出力される際に、ログメモリ 253 に格納されているライセンス I D (L I D) と L B A とによってセキュアデータ記憶部 250 における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

【0093】

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

【0094】

再び図 6 を参照して、H D 20 のデータ記録部に関して説明する。H D 20 は

、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部 270 を含む。ノーマルデータ記憶部 270 は、データが記憶される円盤状の磁気記録媒体 2701 と、磁気記録媒体 2701 を回転させるモータ 2702 と、モータ 2702 を制御するサーボ制御部 2703 と、磁気記録媒体 2701 上における磁気ヘッドの位置を制御するシーク制御部 2704 と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部 2705 とを含む。

【0095】

HD20 は、さらに、ATA インターフェース部 212 を介して外部との間でデータ授受、制御情報 AC に基づくライセンスの出力に関する判断、およびセキュアデータ記憶部 250 の管理などの HD20 内の動作を制御するためのコントローラ 214 を含む。

【0096】

なお、ノーマルデータ記憶部 270、ATA インターフェース部 212 および端子 210 を除く他の構成は、耐タンパモジュール領域に構成される。

【0097】

図 8 を参照して、ノーマルデータ記憶部 270 の構成は、一般の公知のハードディスクの構成と変わるところはなく、データ記憶部 2700 を含む。データ記憶部 2700 は、領域 2800～280A ($A = \max LBA$ 、 $\max LBA$ は自然数) の各々は、暗号化コンテンツデータおよび暗号化コンテンツデータの付属データ、ライセンステーブル等を格納する。そして、領域 2800～280A に対応して $LBA: 0 \sim \max LBA$ が付与されており、各領域 2800～280A は、 $LBA: 0 \sim \max LBA$ によって指定され、暗号化コンテンツデータ等のデータは、指定された各領域 2800～280A に入出力される。

【0098】

なお、ライセンステーブルは、暗号化コンテンツデータとライセンスの関係を示す情報テーブルであり、ライセンステーブルを参照することで、暗号化コンテンツデータに対応するライセンスと、そのライセンスが記憶されている LBA を特定することができる。したがって、ライセンステーブルは、暗号化コンテンツデータの記憶、削除時、あるいはライセンスの記憶、移動、削除時にその内容が

変更される。

【0099】

したがって、HD20は、LBA：0～maxLBAによって指定できるノーマルデータ記憶部270と、それに続くLBA：maxLBA+1～maxLBA+Lによって指定できるセキュアデータ記憶部250、より具体的には、ライセンスメモリ251に対してデータあるいはライセンスの入出力が行なうことができる。

【0100】

また、ノーマルデータ記憶領域270およびライセンス領域251に対するLBAの値については、本実施の形態に限るものではない。

【0101】

なお、セキュアデータ記憶部250は、通常のアクセスコマンドではATAインタフェース部212を介して、直接、外部からアクセスできない等の手段を設けることで耐タンパ性を確保した、耐タンパ構造を備えている。

【0102】

また、HD20のセキュアデータ記憶部250は、全て半導体メモリによって構成されるものとして説明したが、耐タンパ性を確保した上で、セキュアデータ記憶部250の一部あるいはその全てを、磁気記録媒体2701上に記憶する構成としてもよい。

【0103】

以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0104】

[配信]

まず、図1に示すデータ配信システムにおいて、ライセンス提供装置40から端末装置10に装着されたHD20へライセンスを配信する動作について説明する。

【0105】

図9および図10は、図1に示すデータ配信システムにおいて、端末装置10

のユーザが端末装置 10 から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンスがライセンス提供装置 40 から端末装置 10 に装着された HD 20 へ向けて送信され、HD 20 に記憶される際の処理（配信セッション）を説明するための第 1 および第 2 のフローチャートである。

【0106】

図 9 における処理開始以前に、端末装置 10 のユーザは、端末装置 10 をモデム 106 によりネットワーク 30 に接続し、端末装置 10 をネットワーク 30 を介してライセンス提供装置 40 に接続していることを前提としている。

【0107】

図 9 を参照して、端末装置 10 のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置 10 のコントローラ 108 は、バス BS2 および HD インターフェース部 110 を介して HD 20 へクラス証明書の出力要求を出力する（ステップ S1）。HD 20 のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介してクラス証明書の出力要求を受理すると（ステップ S2）、バス BS3 を介して認証データ保持部 202 からクラス証明書 $Cm1 = KPcm1 // Icm1 // E(Ka, H(KPcm1 // Icm1))$ を読出し、クラス証明書 $Cm1$ を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する（ステップ S3）。

【0108】

端末装置 10 のコントローラ 108 は、HD 20 から HD インターフェース部 110 およびバス BS2 を介してクラス証明書 $Cm1$ を受理すると（ステップ S4）、受理したクラス証明書 $Cm1$ をモデム 106 およびネットワーク 30 を介してライセンス提供装置 40 へ送信する（ステップ S5）。

【0109】

ライセンス提供装置 40 では、端末装置 10 からクラス証明書 $Cm1$ を受信すると（ステップ S6）、受信した $Cm1$ が正当なクラス証明書であるか否かを認証する（ステップ S7）。認証処理は次のように行なわれる。

【0110】

ライセンス提供装置40は、クラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を受理すると、HD20から出力されたクラス証明書 C_{m1} に含まれる署名データ $E(K_a, H(KP_{cm1} // I_{cm1}))$ を認証部418において認証鍵 KPa で復号し、ハッシュ値 $H(KP_{m1} // I_{cm1})$ を抽出する。そして、さらに、認証部418は、クラス証明書 C_{m1} に含まれる $KP_{cm1} // I_{cm1}$ のハッシュ値を演算し、クラス証明書 C_{m1} から抽出したハッシュ値と演算したハッシュ値とを比較する。配信制御部412は、認証部418における復号処理結果から、上記の復号ができ、かつ、2つのハッシュ値の値が一致したと判断すると、HD20から受理したクラス証明書 C_{m1} は、正当な証明書であると判断する。

【0111】

ステップS7において、クラス証明書 C_{m1} が正当な証明書であると判断された場合、配信制御部418は、クラス公開鍵 KP_{cm1} を受理する（ステップS8）。そして、次の処理（ステップS9）へ移行する。正当なクラス証明書でない場合には、クラス証明書 C_{m1} を受理しないでエラー通知を端末装置10へ出力し（図10のステップS44）、端末装置10においてエラー通知が受理されると（図10のステップS45）、配信セッションが終了する。

【0112】

ステップS8においてクラス公開鍵 KP_{cm1} が受理されると、配信制御部412は、ライセンスID（ LID ）を生成し（ステップS9）、さらに制御情報ACを生成する（ステップS10）。そして、セッション鍵発生部414は、配信のためのセッション鍵 $Ks1a$ を生成する（ステップS11）。セッション鍵 $Ks1a$ は、認証部418によって得られたHD20に対応するクラス公開鍵 KP_{cm1} によって、暗号処理部420によって暗号化され、暗号データ $E(KP_{cm1}, Ks1a)$ が生成される（ステップS12）。

【0113】

そして、配信制御部412は、ライセンスID（ LID ）および暗号化されたセッション鍵 $Ks1a$ を1つのデータ列 $LID // E(KP_{cm1}, Ks1a)$ として、バスBS1および通信装置450を介して端末装置10へ向けて出力す

る（ステップS13）。

【0114】

端末装置10は、ネットワーク30を介してLID//E（KPcm1, Ks1a）を受信すると（ステップS14）、受信したLID//E（KPcm1, Ks1a）をHD20へ出力する（ステップS15）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID//E（KPcm1, Ks1a）を受信する（ステップS16）。コントローラ214は、バスBS3を介して受信したE（KPcm1, Ks1a）を復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持されるHD20に固有なクラス秘密鍵Kcm1によって復号処理することにより、セッション鍵Ks1aを復号し、セッション鍵Ks1aを受信する（ステップS17）。

【0115】

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵Ks1aの受信を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵Ks1aが受信された旨の通知を受信すると、HD20にセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS18）。HD20のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受信すると、セッション鍵発生部226に対してセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵Ks2aを生成する（ステップS19）。

【0116】

そして、コントローラ214は、セキュアデータ記憶部250のログメモリ253から最も古いをログが格納されているバンクを検索し、その検索したバンク n ($0 \leq n \leq N-1$) の管理番号領域2541、ライセンスID領域2542、Ks2a領域2543、ST1領域2544に対して、それぞれ、新たな管理番

号、ステップS 16で受理したライセンスID、ステップS 19において生成されたセッション鍵K s 2 a、および”受信待”を格納する(ステップS 20)。したがって、バンクnに格納されるログは最も新しいログとなる。このとき、ログを構成する他の領域については、その内容を初期化、たとえば、全て”0”としてもよいし、そのままの状態であってもよい。

【0117】

ここで、図11を参照して、ステップS 20の詳細な動作について説明する。図11は、ステップS 20の詳細な動作を示すフローチャートである。、コントローラ214は、ステップS 19の後、ログメモリ253のうち、最新のログが記録されているログ領域に対応するバンクn-1を特定し、そのバンクn-1によって指定されるログ領域に格納された履歴情報に含まれる管理番号mを取得する(ステップS 20 a)。

【0118】

図12を参照して、ステップS 20 aの詳細な動作について説明する。図12は、ステップS 20のさらに詳細なフローチャートである。コントローラ214は、ステップS 19の後、変数nに対して領域2532を示すバンク1のバンク番号1を設定し(ステップS 20 c)、バンク0に格納されている管理番号を取得して、変数mに代入する(ステップS 20 d)。そして、コントローラ214は、ログメモリ253のバンクnに格納されている管理番号を取得して、変数maに代入する(ステップS 20 e)、 $ma - m$ を演算して演算結果が”1”であるか否かを判定する(ステップS 20 f)。演算結果が”1”であるとき、コントローラ214は、変数nに、1を加えた $n + 1$ を代入し(ステップS 20 g)、変数maに代入されている管理番号を変数mに代入する(ステップS 20 h)。その後、ステップS 20 e ~ S 20 hが繰返し行なわれる。

【0119】

ステップS 20 fにおいて、コントローラ214は、演算結果が”1”でないとき、バンクn-1が、最新のログが記録されている領域であると判断し、最新の管理番号mの取得を終了し、図11に示すステップS 20 bへ移行する。このとき、最も古いログはバンクnに格納されている。

【0120】

ステップS20fにおいて、演算結果が”1”であると判定された場合に、ステップS20g, S20h, S20e, S20fが、順次、行なわれるのは、演算結果が”1”である場合、変数 m と変数 ma とに代入された管理番号 m と管理番号 ma とが連続した番号であり、バンク $n-1$ とバンク n とに、前後してログが格納されたことを示している。つまり、ログメモリ253の領域はバンク番号順に巡回的に使用され、かつ、管理番号も M の剰余系において巡回的に使用されるのであるから連続して格納された場合、連続するバンクに格納された管理番号の差は”1”となるからである。したがって、バンク $n-1$ には、最新のログが格納されていないことが判る。なお、バンク n については不明である。そして、判断する領域を1つ進めて、バンク n に格納されているログについて判定する。すなわち、バンク n に格納されているログの管理と、次の領域であるバンク $n+1$ に格納されているログの管理番号に基づいて判定する。フローチャートでは、ステップS20gにおいて、 n には $n+1$ が代入されることで次の領域に対する判定となる。

【0121】

このように、ステップS20f, S20g, S20h, S20eのループを繰返し行なうことによってバンク0から順にバンク $N-1$ まで連続した領域に格納された管理番号が連続しているか否かが判定される。なお、バンク $N-1$ と比較されるのはバンク0の番号である、上述したように、バンクの番号に対する演算は N の剰余系においてなされる。すなわち、バンク $N-1$ の判定においては、 $n-1=N-1$ 、 $n=0$ である。

【0122】

ステップS20fにおいて、演算結果が”1”でない場合に、バンク $n-1$ に格納されたログを最新のログと判定するのは、この場合、バンク $n-1$ およびバンク n に格納される2つのログの管理番号が不連続であるからである。すなわち、上述したように、前後してログの管理番号は連続する。逆に連続しない管理番号を含むログは連続しないこととなる。

【0123】

また、図12に従ってバンク $n-1$ を特定するためには、HD20の出荷時におけるログメモリ253の初期化によってログメモリ253の全ての領域2531~253Nに、すなわち、バンク0~バンクN-1に対して、所定の管理番号を含むログを格納しておく必要がある。管理番号として全てのバンクに対して同じ値、あるいは、連続するバンクに連続する値（一ヶ所不連続となる）を持つログを格納しておく。なお、ログの他の領域については、いずれの値であってもよい。

【0124】

再び、図11を参照して、上述した方法によって最新の履歴情報（ログ）が記録されているバンク $n-1$ と、バンク $n-1$ に格納された管理番号 m とを取得した後、コントローラ214は、バンク n に、管理番号 $m+1$ 、ステップS16で受理したライセンスID、ステップS19で受理したセッション鍵 $Ks2a$ を格納し、ST1領域2545のステータスST1を”受信待”に設定する（ステップS20b）。これにより、図9に示すステップS20の動作が終了し、ステップS21へ移行する。

【0125】

再び、図9を参照して、ステップS20の後、暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵 $Ks1a$ によって、切換スイッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵 $Ks2a$ と個別公開鍵 $KPom2$ とからなる1つのデータ列を暗号化し、 $E(Ks1a, Ks2a // KPom2)$ 生成する（ステップS21）。そして、暗号処理部224は、 $E(Ks1a, Ks2a // KPom2)$ をバスBS3に出力する。バスBS3に出力された暗号化データ $E(Ks1a, Ks2a // KPom2)$ は、コントローラ214により受理され、コントローラ214は、受理した暗号化データとライセンスID（LID）とを1つのデータ列としたデータ $LID // E(Ks1a, Ks2a // KPom2)$ をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS22）。

【0126】

そして、端末装置 10 は、データ L I D // E (K s 1 a , K s 2 a // K P o m 2) を H D 20 から受理すると (ステップ S 23)、受理したデータをネットワーク 30 を介してライセンス提供装置 40 に出力する (ステップ S 24)。

【0127】

ライセンス提供装置 40 は、データ L I D // E (K s 1 a , K s 2 a // K P o m 2) を受信すると (ステップ S 25)、復号処理部 422 においてセッション鍵 K s 1 a による復号処理を実行し、H D 20 で生成されたセッション鍵 K s 2 a、および H D 20 の個別公開鍵 K P o m 2 を受理する (ステップ S 26)。

【0128】

配信制御部 412 は、ライセンス I D (L I D) に対応するデータ I D (D I D) およびコンテンツ鍵 K c をコンテンツ DB 402 から取得し (ステップ S 27)、ライセンス I D (L I D) および制御情報 A C と併せた 1 つのデータ列としてのライセンス L I C = K c // A C // D I D // L I D を生成する。

【0129】

配信制御部 412 は、生成したライセンス L I C を暗号処理部 424 に与える。暗号処理部 424 は、復号処理部 422 によって得られた H D 20 の個別公開鍵 K P o m 2 によってライセンス L I C を暗号化して暗号化データ E (K P o m 2 , L I C) を生成する (ステップ S 28)。そして、暗号処理部 426 は、暗号処理部 424 から受ける暗号化データ E (K P o m 2 , L I C) を、復号処理部 422 から受けるセッション鍵 K s 2 a によって暗号化し、暗号化データ E (K s 2 a , E (K P o m 2 , L I C)) を生成する (ステップ S 29)。

【0130】

図 10 を参照して、配信制御部 412 は、バス B S 1 および通信装置 450 を介して暗号化データ E (K s 2 a , E (K P o m 2 , L I C)) を端末装置 10 へ向けて出力する (ステップ S 30)。端末装置 10 は、ネットワーク 30 を介して暗号化データ E (K s 2 a , E (K P o m 2 , L I C)) を受理すると (ステップ S 31)、受理した暗号化データを H D 20 へ出力する (ステップ S 32)。

【0131】

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE (Ks2a, E (KPom2, LIC)) を受理すると (ステップS33)、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE (Ks2a, E (KPom2, LIC)) を復号し、HD20において、ライセンスLICが個別公開鍵KPom2により暗号化された暗号化ライセンスE (KPom2, LIC) が受理される (ステップS34)。そして、復号処理部228は、暗号化ライセンスE (KPom2, LIC) をバスBS3へ出力する。

【0132】

コントローラ214の指示によって、暗号化ライセンスE (KPom2, LIC) は、復号処理部216において個別秘密鍵Kom2によって復号され、ライセンスLICが受理される (ステップS35)。

【0133】

HD20のコントローラ214は、ライセンスLICの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてライセンスLICが受理された旨の通知を受理すると、HD20のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBA (「格納LBA」と呼ぶ。) をバスBS2およびHDインターフェース110を介してHD20へ出力する (ステップS36)。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してライセンスLICの格納LBAを受理すると (ステップS37)、その受理した格納LBAをログメモリ253のバンクnに格納されたログのLBA領域2547に記憶する (ステップS38)。

【0134】

そして、コントローラ214は、受理したライセンスLICに含まれるライセンスID (LID) と、ステップS16において受理したライセンスLID (L

ID)とを比較し、一致しているか否かをチェックする(ステップS39)。コントローラ214は、LIDが一致しており、受理したライセンスLICが正しいものであると判断すると、端末装置10から受理したセキュアデータ記憶部250内のLBAに、受理したライセンスLICを記憶する(ステップS40)。

【0135】

コントローラ214は、指定されたLBAにライセンスLICを記憶すると、有効フラグ領域252のそのLBAに対応するフラグを”有効”にする(ステップS41)。そして、コントローラ214は、さらに、ログメモリ253のバンクnに格納されたログのST1領域2544のステータスST1を”受信済”に変更し(ステップS42)、配信セッションにおける一連の処理が終了したことを端末装置10に通知する。

【0136】

そして、端末装置10において、HD20から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

【0137】

一方、ステップS39において、コントローラ214は、LIDが一致せず、受理したライセンスLICが正しくないと判断すると、エラー通知を端末装置10へ出力し(ステップS43)、端末装置10は、エラー通知を受理すると(ステップS45)、処理を終了する。

【0138】

図9および図10に示された配信処理においては、ライセンス提供装置40におけるログの記録に関する記載がなされていないが、図4に示すように、ライセンス提供装置40には、十分な記憶容量を持つログDB404が備えられており、配信セッションにおける各ステップにおけるログがログDB404に記憶される。また、ログDB404には、ライセンスの送信に伴う課金情報なども記憶される。

【0139】

図9および図10に示された配信処理における一連の処理において、ステップS25からステップS44の処理中に異常が発生して処理が中断したときは、再

書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置 10 の電源が遮断されたり、ライセンス提供装置 40 側の異常、あるいは端末装置 10 とライセンス提供装置 40 との通信異常など、種々の異常ケースが考えられる。ここで、HD 20 内のログメモリ 253 に格納されたステータス ST 2 を除く出力ログの内容がすべて格納されたステップ S 22 終了後からステップ S 44 までの処理中に処理が中断した場合には、HD 20 は、再書込処理を行なってライセンスの提供を受けることが可能である。ここでは、端末装置 10 の判断によって再書込処理を行なうものとしたため、端末装置 10 において処理の進行が確認できるステップ S 22 からステップ S 24 を除く、ステップ S 25 からステップ S 44 の処理中に処理が中断した場合を再書込処理の対象とし、他のステップにおける処理の中断においてはライセンス提供装置 40 からライセンスの提供がなされなかったものと判断し、図 9 および図 10 に示したフローチャートに従って、最初から処理を行なうこととした。

【0140】

同様に、ライセンス提供装置 40 がライセンスを出力するまでのライセンス提供装置 40 内のステップ S 25 からステップ S 30 までの処理については、端末装置 10 において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図 9 および図 10 に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

【0141】

[配信における再書込]

図 13～図 15 は、図 9 および図 10 において示した配信処理におけるステップ S 25 からステップ S 44 の処理中に異常が発生したときに行なわれる再書込処理の第 1 から第 3 のフローチャートであり、図 16 は、図 13 のステップ S 112 a の詳細な動作を説明するためのフローチャートである。

【0142】

図 13 を参照して、端末装置 10 は、ステップ S 25 からステップ S 44 の処理中に異常が発生したと判断すると、ライセンス LIC の LID // 再書込要求をネットワーク 30 を介してライセンス提供装置 40 へ出力する（ステップ S 1

01)。配信制御部412は、通信装置450およびバスBS1を介してLID／／再書込要求を受理すると（ステップS102）、セッション鍵発生部414にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部414は、再書込処理のためのセッションキー鍵Ks1bを生成する（ステップS103）。そして、配信制御部412は、このセッションにおいてHD20とやり取りしたログが格納されているログDB402からHD20に対応するクラス公開鍵KPcm1を取得し（ステップS104）、暗号処理部420に与える。クラス公開鍵KPcm1を受けた暗号処理部420は、クラス公開鍵KPcm1をによりセッション鍵Ks1bを暗号化し、E（KPcm1, Ks1b）が生成される（ステップS105）。そして、配信制御部412は、LID／／E（KPcm1, Ks1b）をバスBS1および通信装置450を介して端末装置10へ向けて出力する（ステップS106）。

【0143】

端末装置10は、ネットワーク30を介してLID／／E（KPcm1, Ks1b）を受理すると（ステップS107）、受理したLID／／E（KPcm1, Ks1b）をHD20へ出力する（ステップS108）。そして、HD20のコントローラ214は、端子210およびATAインターフェース部212を介してLID／／E（KPcm1, Ks1b）を受理する（ステップS109）。コントローラ214は、受理したE（KPcm1, Ks1b）をバスBS3を介して復号処理部230へ与え、復号処理部230は、Kcm保持部204に保持されるHD20に固有なクラス秘密鍵Kcm1によって復号処理することにより、セッション鍵Ks1bを復号し、セッション鍵Ks1bが受理される（ステップS110）。

【0144】

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵Ks1bの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵Ks1bが受理された旨の通知を受理すると、ログの

出力要求をバスBS2およびHDインターフェース部110を介してHD20へ出力する(ステップS111)。

【0145】

HD20のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理し(ステップS112)、ログの複製処理を行なう(ステップS112a)。

【0146】

ここで、図16を参照して、ステップS112aの詳細な動作について説明する。コントローラ214は、ログメモリ253のうち、最新のログが格納されたバンク $n-1$ の特定と、バンク $n-1$ に格納されているログの管理番号 m とを取得する(ステップS112b)。このステップS112bの詳細な動作は、図11および図12に示すフローチャートに従って行なわれる。

【0147】

ステップS112bの後、コントローラ214は、変数 k (k は自然数、 $1 \leq k \leq N$)に"1"を、変数ERRに"偽"を代入し(ステップS112c)、バンク $n-k$ に格納されたログのライセンスID(LID)が、ステップS109で受理したライセンスID(LID)に一致するか否かを判定する。すなわち、コントローラ214は、ステップS112bで検出した最新のログに格納されたライセンスID(LID)が、ステップS109で受理したライセンスID(LID)に一致するか否かを判定する。

【0148】

2つのライセンスID(LID)が不一致である場合、コントローラ214は、 k が N (バンクの総数)よりも小さいか否かを判定し(ステップS112e)、 k が N 以上であるとき、全てのバンクに対して確認が終了し、つまり、受理したライセンスID(LID)に一致するLIDを記録したログが格納されていないことが確認され、ステップS112hへ進み、変数ERRに"真"を代入する(ステップS112h)。そして、図13のステップS113aに戻り、変数ERRを確認する。

【0149】

再び、図13を参照して、コントローラ214は、変数ERRを確認する（ステップS113a）。図16のステップS112hから移行した場合、変数ERRは”真”であり、該当するライセンスIDを記録するログが、ログメモリ253に格納されていなかったことを示しているので処理を継続することはできない。したがって、図15に示すステップS160へ移行し、エラー通知を端末装置10へ出力する（ステップS160）。そして、端末装置10は、エラー通知を受理し（ステップS161）、書込拒否により一連の動作が終了する。

【0150】

図16を参照して、ステップS112eにおいて、コントローラ214は、 k は N よりも小さいと判定すると、全てのバンクに対する確認が終了していないので、今、確認したログより、1つ古いログを確認するために、変数 k に $k-1$ を代入する（ステップS112f）、ステップS112dへ移行する。そして、コントローラ214は、バンク $n-k$ に格納されたライセンスID（LID）が、ステップS109で受理したライセンスID（LID）と一致するか否かを判定する。この場合、変数 k の値は”2”であるので、コントローラ214は、バンク $n-2$ に格納されたログのライセンスID（LID）が、ステップS109で受理したライセンスID（LID）に一致するか否かを判定する。そして、2つのライセンスID（LID）が不一致である場合、ステップS112e、S112f、S112dが行なわれる。

【0151】

このように、コントローラ214は、最新のログから、より古いログが格納されるバンクへ向けて、各バンクに格納されたライセンスID（LID）が、ステップS109で受理したライセンスID（LID）と一致するか否かを判定する。そして、この動作（ステップS112e、S112f、S112d）は、ステップS109で受理したライセンスID（LID）に一致するライセンスID（LID）が検出されるまで、あるいは、全てのバンクの確認が終了するまで繰返し行なわれる。なお、バンク番号は N の剰余系であるので、ライセンスIDの確認は、バンク $n-1$ （ $k=1$ ）、 $n-2$ （ $k=2$ ）、 \dots 、 1 （ $k=n-1$ ）、 0 （ $k=n$ ）、 $N-1$ （ $k=n+1$ ）、 \dots 、 n （ $k=N$ ）の順に確認され

る。

【0152】

ステップS112dにおいて、2つのライセンスID (LID) が一致したとき、コントローラ214は、バンクn-kに格納されたログを取得し、その取得したログの管理番号mをm+1に変更した後、そのログをバンクnに格納する (ステップS112g)。つまり、コントローラ214は、ライセンス提供装置40から送信されたライセンスID (LID) に一致するライセンスID (LID) を含むログがログメモリ253に格納されている場合、そのログ (複数有る場合は、より新しいログ) を、最も古いログが格納されたバンクnに複製する。この場合、管理番号のみは複製されず、複製したログが新しいログとして扱われるよう先のバンクn-1に格納されたログの管理番号に1を加えた値を記録する。したがって、最も古いログは削除され、そこに、現在、進行中の再書込処理に対する新たなログが格納される。

【0153】

その後、図13に示すステップS113aへ移行する。

再び、図13を参照して、コントローラ214は、変数ERRを格納する (ステップS133a)。図16に示すステップS112gから移行した場合、変数ERRは”偽”であり、該当するライセンスIDを記録したログがバンクnに複製されるので処理の継続が可能であると判断され、ステップS113へ移行して、ログメモリ253のバンクnに格納された格納LBAに記憶されるライセンスLICのライセンスID (LID) と、ログメモリ253に格納されたライセンスID (LID) とが一致するか否かをチェックする (ステップS113)。

【0154】

コントローラ214は、両ライセンスID (LID) が一致すると判断すると、配信処理としては、ライセンス提供装置40からのライセンスLICの受理までは行なわれ、HD20においてライセンスLICは受理していると認識する。そうすると、コントローラ214は、ログメモリ253のバンクnに格納された格納LBAにより指定された領域に記憶されるライセンスに対応する有効フラグ領域252に格納されているフラグをチェックして、そのライセンスの有効性を

チェックする（ステップS114）。

【0155】

コントローラ214は、ライセンスが有効であると判断すると、ログメモリ253のバンクnに格納されたログのステータスST2を”データ有”に変更し、次の処理（ステップS118）へ移行する。一方、コントローラ214は、ステップS114においてライセンスが無効であると判断すると、ログメモリ253のバンクnに格納されたログのステータスST2を”移動済”に変更し、次の処理（ステップS118）へ移行する。

【0156】

ステップ113において、コントローラ214は、比較したライセンスID（LID）が一致しないと判断したときは、ログメモリ253のバンクnに格納されたログのステータスST2を”データ無”に変更する（ステップS117）。

【0157】

ステータスST2の変更処理がなされると、コントローラ214は、ログメモリ253のバンクnからライセンスID（LID）、ステータスST1、ST2およびセッション鍵Ks2cを取得する（ステップS118）。ここで、この処理は図9および図10のフローチャートに従って配信セッションの中断に対する処理であるためログメモリ253のバンクnに格納されているセッション鍵はKs2aであるが、説明の関係上、ログメモリ253のバンクnから取得したセッション鍵をKs2cとしている。そして、コントローラ214は、取得したセッション鍵Ks2cをバスBS3を介して暗号処理部224へ出力する。

【0158】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したセッション鍵Ks2cを暗号化し、E（Ks1b, Ks2c）生成する（ステップS119）。そして、暗号処理部224は、生成したE（Ks1b, Ks2c）をバスBS3に出力する。バスBS3に出力されたE（Ks1b, Ks2c）は、コントローラ214により受理され、コントローラ214は、ステップS118において取得したデータとともに1つのデータ列LID／／E（Ks1b, Ks

2c) //ST1//ST2を生成し、ハッシュ関数を用いてハッシュ値H (LID//E (Ks1b, Ks2c) //ST1//ST2)を生成する(ステップS120)。そして、コントローラ214は、ハッシュ値H (LID//E (Ks1b, Ks2c) //ST1//ST2)をバスBS3を介して暗号処理部224へ出力する。

【0159】

暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1bによって、バスBS3から取得したハッシュ値H (LID//E (Ks1b, Ks2c) //ST1//ST2)を暗号化し、E (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))生成する(ステップS121)。そして、暗号処理部224は、生成したE (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))をバスBS3に出力する。ここで、データ列LID//E (Ks1b, Ks2c) //ST1//ST2を受信ログと称し、E (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))は、受信ログに対してセッション鍵Ks1bを用いて電子署名を行なった署名データである。また、ログメモリ253に格納されていたセッション鍵Ks2cをセッション鍵Ks1bを用いて暗号化するのは、セッション鍵Ks2cの漏洩によるライセンスの流出の危険性を排除するためである。

【0160】

コントローラ214は、バスBS3から署名データを受理すると、ステップS118において取得した受信ログを用いて、署名付き受信ログLID//E (Ks1b, Ks2c) //ST1//ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c) //ST1//ST2))を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS122)。

【0161】

端末装置10は、署名付き受信ログLID//E (Ks1b, Ks2c) //ST1//ST2//E (Ks1b, H (LID//E (Ks1b, Ks2c)

／／ST1／／ST2))をHD20から受理すると(ステップS123)、受理したデータをネットワーク30を介してライセンス提供装置40へ出力する(ステップS124)。そして、ライセンス提供装置40は、ネットワーク30を介して署名付き受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2／／E(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を受信する。(ステップS125)

図14を参照して、ライセンス提供装置40は、受信した署名付き受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2／／E(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))の検証を行なう(ステップS126)。検証処理は次のように行なわれる。

【0162】

配信制御部412は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データE(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を復号処理部422へ出力するとともに、セッション鍵発生部414にセッション鍵Ks1bを発生するように指示する。そして、復号処理部422は、セッション鍵Ks1bによって署名データE(Ks1b, H(LID／／E(Ks1b, Ks2c)／／ST1／／ST2))を復号し、HD20にて演算したハッシュ値を抽出する。一方、配信制御部412は、署名付き受信ログの前半部である受信ログLID／／E(Ks1b, Ks2c)／／ST1／／ST2のハッシュ値を演算し、復号処理部422により復号されたHD20で演算されたハッシュ値と比較する。配信制御部412は、2つのハッシュ値が一致したと判断すると、HD20から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置40において承認される。

【0163】

ステップS126においてHD20から受理した署名付き受信ログが承認されると、配信制御部412は、受理したライセンスID(LID)に基づいてログDB404を検索する(ステップS127)。配信制御部412は、受理したライセンスID(LID)がログDB404内に格納されており、HD20に対して確かに提供を行なったライセンスであると判断すると、受理したステータスS

T1, ST2の内容を確認する(ステップS128)。

【0164】

配信制御部412は、ステータスST1が”受信待”であり、ステータスST2が”データ無”であるとき、HD20に送信したはずのライセンスLICが何らかの異常によりHD20において受理されていないと判断し、受信したデータ列に含まれる暗号化データE(Ks1b, Ks2c)を復号処理部422へ出力してセッション鍵Ks1bによってセッション鍵Ks2cを復号する。そして、復号されたセッション鍵Ks2cは、バスBS1を介して配信制御部412へ出力され、配信制御部412においてセッション鍵Ks2cが受理される(ステップS129)。

【0165】

そして、配信制御部412は、異常発生時のセッション鍵Ks2aを今回受理したセッション鍵Ks2cと比較チェックする(ステップS130)。配信制御部412は、セッション鍵Ks2aとセッション鍵Ks2cとが一致していると判断すると、ライセンスLICの再書込に対する許可通知を端末装置10へ出力する(ステップS133)。

【0166】

一方、ステップS126においてHD20から受理したデータ列が承認されなかったとき、ステップS127においてHD20から受理したライセンスID(LLID)がログDB404内に格納されておらず、HD20に対して提供を行なったライセンスであると判断できないとき、ステップS128において、HD20においてライセンスLICが受理されたものと判断されたとき、またはステップS130において、セッション鍵Ks2aがセッション鍵Ks2cと一致しないと判断されたときは、配信制御部412は、ライセンスの再送信は不可と判断し、バスBS1および通信装置450を介してエラー通知を端末装置10へ向け出力し(ステップS131)、端末装置10は、ネットワーク30を介してエラー通知を受理すると(ステップS132)、処理が終了する。すなわち、ライセンス提供装置40において、ライセンスの再書込が拒否されて処理が終了する。

。

【0167】

端末装置10のコントローラ108は、ステップS133においてライセンス提供装置40が出力した許可通知を受理すると（ステップS134）、HD20に対するセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS135）。

【0168】

HD20は、ライセンス提供装置40からの再書込処理許可通知に基づいて、端末装置10からセッション鍵の生成要求通知を受理すると、新たにセッション鍵Ks2bを生成し（ステップS136）、ログメモリ253のバンクnのログに記録されているセッション鍵Ks2c（=Ks2a）を、生成したセッション鍵Ks2bに、ログのステータスST1を”受信待”に変更する（ステップS137）。

【0169】

以下、ステップS138からの一連の処理は、図9および図10において説明したステップS21から処理終了までの一連の処理において、セッションKs2aに代えて新たに生成してセッション鍵Ks2bが使用される他は、同様の処理が行なわれる。したがって、ステップS138からの一連の処理の説明は繰返しになるので省略する。

【0170】

なお、図13～図15のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップS101～S131、ステップS133およびステップS142～S160のいずれかのステップにおいて処理が中断した場合には、再び図13～図15のフローチャートに従って再書込処理を行なうことができる。一方、ステップS134～S141のいずれかのステップにおいて処理が中断した場合には、図9および図10のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

【0171】

このようにして、端末装置10に装着されたHD20が正規のクラス証明書C

m1 を保持する機器であることを確認したうえで、クラス証明書 C_{m1} に含まれて送信されたクラス公開鍵 KP_{cm1} によってライセンス提供装置 40 および HD20 でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

【0172】

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置である HD20 における署名付き受信ログをライセンス提供装置 40 へ送信することで、ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

【0173】

[複製・移動]

図17は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図17を参照して、端末装置10にデータ記憶装置として2台のHD20, 21が装着可能であり、端末装置10を介してHD20からHD21へライセンスの複製または移動が行なわれる。

【0174】

ここで、HD21は、HD20と異なるデータ記憶装置であるため、HD20とは異なる個別公開鍵 KP_{om5} と個別秘密鍵 K_{om5} とを保持している。この場合、HD21における識別子 z は、HD20の $z=2$ とは異なる $z=5$ となる。また、HD21のクラスは、HD20のクラスと同じ $y=1$ として以下説明する。すなわち、HD20、HD21とも、クラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, KP_{cm1} // I_{cm1})$ およびクラス秘密鍵 K_{cm1} を保持する。しかしながら、HD21のクラスがHD20のクラスと異なる ($y \neq 1$) 場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、HD20とは異なったものとなる。

【0175】

図18および図19は、図17に示すライセンスの複製・移動が可能なシステムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置10を介して端末装置10に装着されたHD20からHD21へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための第1および第2のフローチャートである。

【0176】

図18を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置10のコントローラ108は、バスBS2およびHDインターフェース部110を介してHD21へクラス証明書の出力要求を出力する（ステップS201）。HD21においては、端子210およびATAインターフェース部212を介してクラス証明書の出力要求が受理されると（ステップS202）、コントローラ214は、認証データ保持部202からクラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を読み出し、クラス証明書 C_{m1} をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS203）。

【0177】

端末装置10は、HD21からクラス証明書 C_{m1} を受理すると（ステップS204）、受理したクラス証明書 C_{m1} をHD20へ送信する（ステップS205）。

【0178】

HD20では、端末装置10からHD21のクラス証明書 C_{m1} を受理すると（ステップS206）、認証部220およびコントローラ214によって受理したHD21のクラス証明書 C_{m1} が正当なクラス証明書であるか否かを認証する（ステップS207）。認証処理は、ライセンス提供装置40における認証処理（図9のステップS7）と同一であるため詳細な説明は省略する。

【0179】

ステップS 207において、コントローラ214は、正当なHD 21のクラス証明書でないと判定した場合には、HD 21のクラス証明書Cm1を非承認として受理せず、エラー通知を端末装置10へ出力する（図19のステップS 252）。そして、端末装置10においてエラー通知が受理されると（図15のステップS 253）、配信セッションが終了する。

【0180】

ステップS 207において、HD 21のクラス証明書Cm1が正当な証明書であると判断されると、HD 20のコントローラ214は、HD 21のクラス証明書Cm1を承認し、セッション鍵Ks1aを生成するようにセッション鍵発生部226を制御し、セッション鍵発生部226は、セッション鍵Ks1aを生成する（ステップS 209）。

【0181】

セッション鍵Ks1aは、認証部220によって得られたHD 21のクラス公開鍵KPcm1によって、暗号処理部222において暗号化され、暗号化データE（KPcm1, Ks1a）が生成される（ステップS 210）。

【0182】

そして、コントローラ214は、暗号化データE（KPcm1, Ks1a）を、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS 211）。

【0183】

端末装置10は、暗号化データE（KPcm1, Ks1a）を受理すると（ステップS 212）、受理した暗号化データE（KPcm1, Ks1a）をHD 21へ出力する（ステップS 213）。ここで、ライセンスID（LID）は、事前に管理ファイルを参照することで端末装置10が取得している。管理ファイルは、HD 20に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部270に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

【0184】

そして、HD 21においては、コントローラ 214が、端子 210およびATAインターフェース部 212を介してLID//E (KP cm1, Ks1a)を受理する(ステップS 214)。続いて、コントローラ 214は、バスBS 3を介してE (KP cm1, Ks1a)を復号処理部 230へ与え、復号処理部 230は、K cm保持部 204に保持されるHD 21に固有なクラス秘密鍵K cm1によって復号処理することにより、セッション鍵Ks1aを復号し、セッション鍵Ks1aを受理する(ステップS 215)。

【0185】

HD 21のコントローラ 214は、HD 20で生成されたセッション鍵Ks1aの受理を確認すると、ATAインターフェース部 212および端子 210を介してその旨を端末装置 10に通知する。端末装置 10は、HD 21においてセッション鍵Ks1aが受理された旨の通知を受理すると、セッション鍵の生成の要求通知をHD 21へ出力する(ステップS 216)。HD 21のコントローラ 214は、端子 210およびATAコントローラ 212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部 226に対してセッション鍵の生成を指示する。そして、セッション鍵発生部 226は、セッション鍵Ks2aを生成する(ステップS 217)。

【0186】

セッション鍵発生部 226は、セッション鍵Ks2aを生成すると、バスBS 3を介してコントローラ 214へ出力し、コントローラ 214は、セッション鍵Ks2aを受ける。そして、コントローラ 214は、最も古いログを格納したバンクを検索し、そこに処理中のセッションに対するログを新たに格納する(ステップS 218)。ステップS 218の詳細な動作は、図 11および図 12に示すフローチャートに従って行なわれる。ただし、HD 21における処理と、HD 20における同様の処理結果を区別するために最も古いログを格納したバンクは、バンクnaであるとする。すなわち、図 11および図 12に示すフローチャートにおける変数nを変数naと読替えればよい。

【0187】

したがって、ログメモリ 253のバンクnaに、バンクna-1に格納される

ログの管理番号に1を加えた新しい管理番号と、ステップS214において受理したライセンスID (LID) とセッション鍵Ks2aとを格納し、ステータスST1を”受信待”にする。

【0188】

続いて、HD21においては、続いて、暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵Ks1aによって、切換スイッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵Ks2aと個別公開鍵K Pom5とからなる1つのデータ列を暗号化し、E (Ks1a, Ks2a//K Pom5) を生成する (ステップS219)。そして、暗号処理部224は、E (Ks1a, Ks2a//K Pom5) をバスBS3に出力する。バスBS3に出力された暗号化データE (Ks1a, Ks2a//K Pom5) は、コントローラ214により受理され、コントローラ214は、受理した暗号化データとライセンスID (LID) とを1つのデータ列としたデータLID//E (Ks1a, Ks2a//K Pom5) をATAインターフェース部212および端子210を介して端末装置10へ出力する (ステップS220)。

【0189】

そして、端末装置10は、データLID//E (Ks1a, Ks2a//K Pom5) をHD21から受理すると (ステップS221)、受理したデータをHD20へ出力する (ステップS222)。

【0190】

HD20では、端子210およびATAインターフェース部110を介してデータLID//E (Ks1a, Ks2a//K Pom5) を受理すると (ステップS223)、復号処理部228においてセッション鍵Ks1aによる復号処理を実行し、HD21で生成されたセッション鍵Ks2a、およびHD21の個別公開鍵K Pom5を抽出して受理する (ステップS224)。そして、復号処理部228は、復号したセッション鍵Ks2aをバスBS3を介してコントローラ214へ出力し、コントローラ214は、セッション鍵Ks2aを受ける。そして、コントローラ214は、最も古いログを格納したバンクに、処理中のセッショ

ンに対するログを新たに格納する（ステップS225）。ステップS225の詳細な動作は、図20に示すフローチャートに従って行なわれる。図20を参照して、ステップS225は、ログメモリ253の最新ログが記録されたバンク $n-1$ を特定し、かつ、バンク $n-1$ に格納された管理番号 m を取得するステップS225aと、バンク n に、管理番号 $m+1$ 、ライセンスID（LID）、セッション鍵 $Ks2a$ 、およびクラス公開鍵 $KPcm y$ を格納し、かつ、ステータス領域を“送信待”に設定するステップS225bとから成る。そして、ステップS225aの詳細な動作は、図12に示すフローチャートに従って行なわれる。したがって、コントローラ214は、図20および図12に示すフローチャートに従って、ステップS223において受理したライセンスID（LID）とステップS224で受理したセッション鍵 $Ks2a$ とをバンク n に格納し、ステータスST1を“送信待”にする。

【0191】

HD20では、ステップS225の処理を終えると、HD20のコントローラ214は、その旨をATAインターフェース部212および端子210を介して端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20からの通知を受理すると、HD20のセキュアデータ記憶部250において、HD20からHD21へ送信するライセンスLICが格納されているLBA（格納LBA）をバスBS2およびHDインターフェース110を介してHD20へ出力する（ステップS226）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介して送信対象のライセンスLICの格納LBAを受理すると（ステップS227）、その受理した格納LBAをセキュアデータ記憶部250のログメモリ253のバンク n に記憶する（ステップS228）。

【0192】

そして、コントローラ214は、受理した格納LBAに格納されるライセンスLICに対応する有効フラグ領域252のフラグが“有効”であるか“無効”であるかを確認する（ステップS229）。コントローラ214は、有効フラグが“有効”であると、格納LBAに格納されているライセンスLICを取得する（

ステップS230)。

【0193】

図19を参照して、HD20では、コントローラ214が、対象のライセンスLICを取得すると、ライセンスLICに含まれるライセンスID(LID)と、ステップS223において受理し、ログメモリ253のバンクnaに格納されているログに記憶されているライセンスID(LID)とを比較し、一致しているか否かをチェックする(ステップS231)。コントローラ214は、一致していると判断すると、取得したライセンスLICに含まれる制御情報ACを確認して利用制限がかけられていないかをチェックする(ステップS232)。

【0194】

コントローラ214は、制御情報ACにおいてライセンスLICの利用が禁止されていないことを確認すると、取得したライセンスLICを暗号処理部232に与える。暗号処理部232は、復号処理部228によって得られたHD21の個別公開鍵KPom5によってライセンスLICを暗号化して暗号化データE(KPom5, LIC)を生成する(ステップS233)。そして、暗号処理部232は、暗号化データE(KPom5, LIC)を切替スイッチPcを介して暗号処理部224へ出力し、暗号処理部224は、暗号処理部232から受けた暗号化データを復号処理部228から受けたセッション鍵Ks2aによって暗号化し、暗号化データE(Ks2a, E(KPom5, LIC))を生成する(ステップS234)。

【0195】

続いて、コントローラ214は、対象のライセンスLICに含まれる制御情報ACに基づいて、HD20からHD21へのライセンスLICの送信が「移動」であるか「複製」であるかを確認する(ステップS235)。コントローラ214は、「移動」であると確認したときは、その対象のライセンスLICに対応する、すなわち、格納LBAに対応する有効フラグ領域252のフラグを“無効”に変更する(ステップS236)。一方、コントローラ214は、「複製」であると確認したときには、当該ライセンスLICがHD20に残っていてもよいので、有効フラグ領域252のフラグの変更は行わずに次の処理(ステップS2

37) へ移行する。

【0196】

コントローラ214は、有効フラグ領域252の処理が終わると、ログメモリ253のバンクnに格納されているログのステータスST1を“送信済”に変更し（ステップS237）、ATAインターフェース部212および端子210を介して暗号化データE（Ks2a, E（KPom5, LIC））を端末装置10へ送信する（ステップS238）。

【0197】

一方、ステップS229において受理した格納LBAに対応する有効フラグ領域252のフラグが“無効”であったとき、ステップS231においてライセンスID（LID）が一致しないとき、または、ステップS232において、取得したライセンスLICに含まれる制御情報ACにより当該ライセンスLICの利用が禁止されているときは、コントローラ214は、端末装置10に対してエラー通知を出力し（ステップS252）、端末装置10においてエラー通知が受理されると（ステップS253）、処理が終了する。

【0198】

端末装置10は、ステップS238においてHD20から出力された暗号化データE（Ks2a, E（KPom5, LIC））を受理すると（ステップS239）、受理した暗号化データをHD21へ出力する（ステップS240）。

【0199】

HD21では、コントローラ214が、端子210およびATAインターフェース部212を介して暗号化データE（Ks2a, E（KPom5, LIC））を受理し（ステップS241）、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE（Ks2a, E（KPom5, LIC））を復号し、HD21において、ライセンスLICが個別公開鍵KPom5により暗号化された暗号化ライセンスE（KPom5, LIC）が受理される（ステップS242）。そして、復号処理部228は、暗号化ライセンスE（KPom5, LIC）をバスBS3へ出力する。

【0200】

コントローラ214の指示によって、暗号化ライセンスE (K P o m 5, L I C) は、復号処理部216において個別秘密鍵K o m 5によって復号され、HD 21においてライセンスL I Cが受理される (ステップS 2 4 3)。

【0201】

コントローラ214は、ライセンスL I Cの受理を確認すると、A T Aインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスB S 2を介して、HD 21においてライセンスL I Cが受理された旨の通知を受理すると、HD 21のセキュアデータ記憶部250において、その受信したライセンスL I Cを格納するL B A (格納L B A) をバスB S 2およびHDインターフェース110を介してHD 21へ出力する (ステップS 2 4 4)。HD 21のコントローラ214は、端子210およびA T Aインターフェース部212を介してライセンスL I Cを格納する格納L B Aを受理すると (ステップS 2 4 5)、その受理した格納L B Aをログメモリ253のバンク n に格納されるログのL B A領域2544に記録する (ステップS 2 4 6)。

【0202】

そして、コントローラ214は、受理したライセンスL I Cに含まれるライセンスID (L I D) と、ステップS 2 1 4において受理したライセンスL I D (L I D) とを比較し、一致しているか否かをチェックする (ステップS 2 4 7)。コントローラ214は、L I Dが一致しており、受理したライセンスL I Cが正しいものであると判断すると、端末装置10から受理したセキュアデータ記憶部250内の格納L B Aに対応する領域に、受理したライセンスL I Cを記憶する (ステップS 2 4 8)。

【0203】

コントローラ214は、指定された格納L B AにライセンスL I Cを記憶すると、有効フラグ領域252のその格納L B Aに対応するフラグを“有効”にする (ステップS 2 4 9)。そして、コントローラ214は、さらに、ログメモリ253のバンク n に格納されたログのステータスS T 1を“受信済”にし (ステッ

プ S 2 5 0)、複製・移動セッションにおける一連の処理が終了したことを A T A インターフェース部 2 1 2 および端子 2 1 0 を介して端末装置 1 0 に通知する。

【0204】

そして、端末装置 1 0 において、H D 2 1 からの処理終了通知が受理されると、H D 2 0 から H D 2 1 へのライセンス L I C の複製・移動セッションが正常終了する。

【0205】

一方、ステップ S 2 4 7 において、H D 2 0 のコントローラ 2 1 4 が、L I D が一致しておらず、受理したライセンス L I C が正しくないと判断すると、A T A インターフェース部 2 1 2 および端子 2 1 0 を介してエラー通知を端末装置 1 0 へ出力し(ステップ S 2 5 1)、端末装置 1 0 においてエラー通知が受理されると(ステップ S 2 5 3)、H D 2 0 から H D 2 1 へのライセンス L I C の複製・移動セッションが異常終了する。

【0206】

ここで、配信セッションのときと同様に、図 1 8 および図 1 9 に示された複製・移動セッションにおける一連の処理において、ステップ S 2 2 7 からステップ S 2 5 2 の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

【0207】

ここで、図 1 8 および図 1 9 に示された複製・移動セッションにおいて、ステップ S 2 2 7 からステップ S 2 3 5 までの処理を再書込処理の対象としたのは、この一連の処理が H D 2 0 の内部処理であり、ステップ S 2 2 6 の終了後は、ステップ S 2 3 8 まで端末装置 1 0 においていずれのステップを処理中に処理が中断したかを特定できないため、すべてステップ S 2 3 6 が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

【0208】

そして、ステップ S 2 3 6 からステップ S 2 4 7 までの処理を再書込処理の対象としたのは、「移動」の場合、この間は、H D 2 0 内のライセンスがステップ

S 2 3 6において無効化され、かつ、HD 2 1内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。

【0209】

また、ステップS 2 4 8からステップS 2 5 0までの処理を再書込処理の対象としたのは、ステップS 2 4 9, S 2 5 0については、これらの処理はステップS 2 4 8におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置10からはステップS 2 4 8の終了が特定できないため、ステップS 2 4 8が終了していないものとみなして、ステップS 2 4 8からステップS 2 5 0を再書込処理の対象としたものである。なお、ステップS 2 4 8が終了していて再書込処理が行なわれた場合には、再書込は拒否される。

【0210】

また、ステップS 2 5 1の処理を再書込処理の対象としたのは、本来、この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置10においては、ステップS 2 5 1において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

【0211】

なお、端末装置10において、上述したように当該セッションがライセンスの「複製」であると判断できる場合、あるいはステップS 2 2 7からステップS 2 3 5およびステップS 2 4 9からステップS 2 5 1のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図18および図19に示された複製・移動セッションを再度実行すればよい。

【0212】

[移動／複製における再書込]

図21～図23は、図18および図19において示した複製・移動セッションの処理フローにおけるステップS 2 2 7からステップS 2 5 2の処理中に異常が発生したときに行なわれる再書込処理の第1から第3のフローチャートである。

【0213】

図21を参照して、端末装置10は、ステップS227からステップS252の処理中に異常が発生したと判断すると、ライセンスID (LID) とライセンスLICの再送要求とをデータ列LID//再送要求としてHD20へ出力する(ステップS301)。HD20では、コントローラ214が、端子210およびATAインターフェース部212を介してLID//再送要求を受理する(ステップS301a)。そして、ログの複製処理を行なう(301b)。複製処理では、ログメモリ253内にステップS301aにおいて受理したLIDを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ253の最も古いログを格納しているバンクnに、検索されたLIDを含むログを複製し、変数ERR=“偽”とする。一方、ログメモリ253内にステップS301aにおいて受理したLIDを含むログが格納されていない場合には、変数ERR=“真”とする。この複製処理の詳細な動作は、図16に示すフローチャートに従って行なわれる。

【0214】

そして、コントローラ214は、ステップS301aの処理結果の判定、すなわち、変数ERRが“真”、“偽”のいずれであるかを判定する(ステップS301b)。“真”の場合、受理したLIDを含むログがバンクnへ複製されたことを示すので、再送要求に対する処理を開始するために次のステップS302へ移行する。“偽”の場合、受理したLIDを含むログがログメモリ253に格納されていなかった、つまり、HD20において受理したLIDによって特定されるライセンスLICの入出力処理がなされていなかったことを示すので、再送要求に対応不能と判断し、図23のステップS372へ移行し、エラー通知を端末装置10に対して出力する。端末装置10においてはエラー通知が受理されると(ステップS373)、処理が終了する。

【0215】

HD20において、ステップS301bにおいて変数ERR=“偽”を確認すると、コントローラ214は、ログメモリ253のバンクnに複製され、かつ、格納されているログのステータスST1の状態を確認する(ステップS302)。コントローラ214は、ステータスST1が“送信待”または“送信済”でな

いとき、すなわち複製・移動セッションにおいてライセンスLICの送信側でないときは、図23に示すステップS371へ処理が移行する。

【0216】

HD20のコントローラ214は、ステータスST1が“送信待”または“送信済”であるときは、セッション鍵発生部226にセッション鍵を生成するように指示し、セッション鍵発生部226は、セッション鍵Ks1aを生成する（ステップS303）。セッション鍵Ks1bが生成されると、コントローラ214は、中断以前に受理した、ライセンスLICの移動／複製先のHD21のクラス公開鍵KPCm1を、ログメモリ253のバンクnに格納されたログから取得する（ステップS304）。ここで、移動／複製先のHD21から再びクラス証明書Imc1を受理することなくログに記憶されるクラス公開鍵KPCm1を用いるのは、再書込処理におけるなりすまし攻撃によるライセンスLICの漏洩を防ぐためである。したがって、再び、クラス証明書Imc1を受理する場合には、HD20において、中断した処理において受理したクラス証明書と再書込処理において受理したクラス証明書とが同一か否かを確認する必要がある。たとえば、再書込処理において受理したクラス証明書Imc1に含まれるクラス公開鍵とログに記録されるクラス公開鍵を比較して再書込処理を行なうか否かを判断する。

【0217】

そして、HD21では、そのクラス公開鍵KPCm1によって、セッション鍵Ks1bが暗号処理部222によって暗号化され、暗号化データE（KPCm1，Ks1b）が生成される（ステップS305）。コントローラ214は、生成された暗号化データE（KPCm1，Ks1b）とライセンスID（LID）とをデータ列LID／／E（KPCm1，Ks1b）としてATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS306）。

【0218】

端末装置10は、LID／／E（KPCm1，Ks1b）を受理すると（ステップS307）、受理したLID／／E（KPCm1，Ks1b）をHD21へ出力する（ステップS308）。

【0219】

HD21において、コントローラ214は、端子210およびATAインターフェース部212を介してLID//E (KPCm1, Ks1b) を受理すると (ステップS309)、バスBS3を介してE (KPCm1, Ks1b) を復号処理部230へ与える。そうすると、復号処理部230は、Kcm保持部204に保持されるHD21に固有なクラス秘密鍵Kcm1によって復号処理を実行してセッション鍵Ks1bを復号し、セッション鍵Ks1bを受理する (ステップS310)。

【0220】

HD21のコントローラ214は、HD20で生成されたセッション鍵Ks1bの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介してHD21からの通知を受理すると、HD21のログメモリ253に格納されるログのHD20への出力要求をバスBS2およびHDインターフェース部110を介してHD21へ出力する (ステップS311)。HD21のコントローラ214は、端子210およびATAコントローラ212を介してログの出力要求通知を受理する (ステップS312)。そして、HD20におけるステップS301aと同様にログの複製処理を行なう (ステップS213a)。複製処理時、ログメモリ253内にステップS309において受理したLIDを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ253の最も古いログを格納しているバンクnaに、検索されたLIDを含むログを複製し、変数ERRa = “偽” とする。一方、ログメモリ253内にステップS309において受理したLIDを含むログが格納されていない場合には、ERRa = “真” とする。このステップS312aの詳細な動作は、図16に示すフローチャートに従って行なわれる。ただし、HD21における処理と、HD20における同様の処理結果を区別するために変数nを変数naとし、変数ERRを変数ERRaとする。すなわち、図16のステップS112bに相当する図12に示すフローチャートにおける変数nを変数naに、変数ERRを変数ERRaにそれぞれ読替えればよい。

【0 2 2 1】

そして、コントローラ 2 1 4 は、ステップ S 3 1 2 a の処理結果の判定、すなわち、ERR a が“真”、“偽”のいずれであるかを判定する（ステップ S 3 2 1 2 b）。“偽”の場合、受理した L I D を含むログがバンク n a へ複製されたことを示すので、再送要求に対する処理を開始するために次のステップ S 3 1 3 へ移行する。“真”の場合、受理した L I D を含むログがログメモリ 2 5 3 に格納されていなかった、つまり、H D 2 1 において、ステップ S 3 1 3 において受理した L I D によって特定されるライセンス L I C の入出力処理がなされなかったことを示すので、再送要求に対応不能と判断し、図 2 3 のステップ S 3 7 1 へ移行し、エラー通知を端末装置 1 0 に対して出力する。端末装置 1 0 においては、エラー通知が受理されると（ステップ S 3 7 3）、処理が終了する。

【0 2 2 2】

H D 2 1 において、ステップ S 3 1 2 b において ERR a = “偽”を確認すると、コントローラ 2 1 4 は、ログメモリ 2 5 3 のバンク n a に格納されているログの格納 L B A に対する領域に記憶されるライセンス L I C のライセンス I D （L I D）と、ログメモリ 2 5 3 のバンク n a に格納されているログのライセンス I D （L I D）とが一致するか否かを確認する（ステップ S 3 1 3）。

【0 2 2 3】

コントローラ 2 1 4 は、ライセンス I D （L I D）が一致すると、さらに、ログメモリ 2 5 3 のバンク n a に格納されているログの格納 L B A に対応する有効フラグ領域 2 5 2 のフラグを確認し、そのライセンス L I C が有効であるか無効であるかを確認する（ステップ S 3 1 4）。コントローラ 2 1 4 は、有効フラグ領域 2 5 2 のフラグが“有効”であるときは、ログメモリ 2 5 3 のバンク n a に格納されているログのステータス S T 2 を“データ有”に変更し（ステップ S 3 1 5）、次の処理（ステップ S 3 1 8）へ移行する。一方、コントローラ 2 1 4 は、有効フラグ領域 2 5 2 のフラグが“無効”であるときは、ログメモリ 2 5 3 のバンク n a に格納されているログのステータス S T 2 を“移動済”に変更し（ステップ S 3 1 6）、次の処理（ステップ S 3 1 8）へ移行する。

【0 2 2 4】

また、コントローラ 214 は、ステップ S313 において両ライセンス ID (LID) が一致しないときは、ログメモリ 253 のバンク n a に格納されているログのステータス ST2 を “データ無” に変更する (ステップ S317)。

【0225】

ステータス ST2 の変更処理がなされると、コントローラ 214 は、ログメモリ 253 のバンク n a からライセンス ID (LID)、ステータス ST1, ST2、セッション鍵 Ks2c および格納 LBA を取得する (ステップ S318)。ここで、この処理は、図 9 および図 10 のフローチャートに従った配信セッションの中断に対する処理であるため、HD21 のログメモリ 253 に格納されている当該処理のログに記憶されているセッション鍵は Ks2a であるが、説明の関係上、ログメモリ 253 のバンク n から取得したセッション鍵を Ks2c としている。そして、コントローラ 214 は、取得したセッション鍵 Ks2c をバス BS3 を介して暗号処理部 224 へ出力する。

【0226】

暗号処理部 224 は、切換スイッチ 260 の接点 P b を介して復号処理部 230 より与えられるセッション鍵 Ks1b によってセッション鍵 Ks2c を暗号化し、 $E(Ks1b, Ks2c)$ 生成する (ステップ S319)。そして、暗号処理部 224 は、生成した $E(Ks1b, Ks2c)$ をバス BS3 に出力する。バス BS3 に出力された $E(Ks1b, Ks2c)$ は、コントローラ 214 により受理され、コントローラ 214 は、ステップ S318 において取得したデータとともに 1 つの受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2$ を生成し、そのハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ を生成する (ステップ S320)。そして、コントローラ 214 は、ハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ をバス BS3 を介して暗号処理部 224 へ出力する。

【0227】

暗号処理部 224 は、切換スイッチ 260 の接点 P b を介して復号処理部 230 より与えられるセッション鍵 Ks1b によって、バス BS3 から取得したハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ を暗号

化し、署名データ $E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ 生成する(ステップS321)。そして、暗号処理部224は、生成した $E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ をバスBS3に出力する。

【0228】

コントローラ214は、バスBS3から署名データを取得すると、ステップS318において取得した受信ログを用いて、署名付き受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2 // E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ を生成し、署名付き受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2 // E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ と格納LBAとを、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS322)。

【0229】

図22を参照して、端末装置10は、署名付き受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2 // E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ と格納LBAとをHD21から受理すると(ステップS323)、受理したデータをHD20へ出力する(ステップS324)。

【0230】

HD20において、コントローラ214は、署名付き受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2 // E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ を受理すると(ステップS325)、受理した署名付き受信ログの検証を行なう(ステップS326)。検証処理は、以下のように行われる。

【0231】

HD20のコントローラ214は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データ $E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ を復号処理部228へ出

力するとともに、セッション鍵発生部226にセッション鍵 K_{s1b} を発生するように指示する。そして、復号処理部228は、セッション鍵 K_{s1b} によって署名データ $E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ を復号し、HD21によって求められたハッシュ値を抽出する。一方、HD20のコントローラ214は、署名付き受信ログの前半部である受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2$ のハッシュ値を演算し、復号処理部228により抽出されたハッシュ値と比較する。HD20のコントローラ214は、2つのハッシュ値が一致したと判断すると、HD21から受理した受信ログは、正当なデータを含むものとしてHD20において承認される。

【0232】

ステップS326において承認されると、HD20のコントローラ214は、ステップS325において承認した受信ログに含まれるライセンスID(LID)をログメモリ253のバンクnに格納されるライセンスID(LID)と比較する(ステップS327)。

【0233】

コントローラ214は、ライセンスID(LID)が一致すると、受信ログに含まれる暗号データ $E(K_{s1b}, K_{s2c})$ を復号処理部228へ出力し、復号処理部228は、セッション鍵発生部226から受けるセッション鍵 K_{s1b} によってセッション鍵 K_{s2c} を復号し、セッション鍵 K_{s2c} が受理される(ステップS328)。そして、復号されたセッション鍵 K_{s2c} は、バスBS3を介してコントローラ214へ出力される。続いて、コントローラ214は、エラー発生時のセッション鍵、すなわち、バンクnのログに記録されているセッション鍵 K_{s2a} と、今回、承認した受信ログに含まれていたセッション鍵 K_{s2c} とを比較する(ステップS329)。コントローラ214は、セッション鍵 K_{s2a} とセッション鍵 K_{s2c} とが一致していると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS330)。

【0234】

HD20のコントローラ214は、受信した受信ログのステータスST1が“

受信待”であり、受信ログのステータスST2が“データ無”であるとき、HD21に送信したはずのライセンスLICが何らかの異常によりHD21において受理されていないと判断する。そうすると、HD20のコントローラ214は、さらに、ログメモリ253のバンクnのログの格納LBAに記憶されるライセンスLICのライセンスID(LID)と、ログメモリ253のバンクnのログのライセンスID(LID)とが一致するか否かを確認する(ステップS331)。HD20のコントローラ214は、ライセンスID(LID)が一致すると、さらに、ログメモリ253のバンクnのログの格納LBAに対応する有効フラグ領域252のフラグを確認し、そのライセンスLICが有効であるか無効であるかを確認する(ステップS332)。そして、コントローラ214は、有効フラグ領域252のフラグが“無効”であるときは、その有効フラグ領域252のフラグを“有効”に変更する(ステップS333)。一方、コントローラ214は、有効フラグ領域252のフラグが“有効”であるときは、次の処理(ステップS334)へ移行する。そして、コントローラ214は、ログメモリ253のバンクnのログの格納LBAと許可通知とをATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS334)。

【0235】

端末装置10のコントローラ108は、HD20からHDインターフェース部110およびバスBS2を介して対象のライセンスLICが格納される格納LBAと許可通知とを受理すると(ステップS335)、HD21に対してセッション鍵の生成の要求通知をバスBS2およびHDインターフェース部110を介してHD21へ出力する(ステップS336)。

【0236】

HD21は、端末装置10からセッション鍵の生成要求通知を受理すると、新たにセッション鍵Ks2bを生成し(ステップS337)、ログメモリ253のバンクnaのログに記憶されているセッション鍵Ks2c(Ks2a)を、生成したセッション鍵Ks2bに、ログのステータスST1を“受信待”に変更する(ステップS338)。

【0237】

以下、ステップ S 3 3 9 からの一連の処理は、図 1 8 および図 1 9 において説明したステップ S 2 1 9 から処理終了までの一連の処理において、セッション鍵 K s 2 a に代えて新たに生成したセッション鍵 K s 2 b が使用される他は、同様の処理が行なわれる。したがって、ステップ S 3 3 9 に続く一連の処理の説明は繰返しになるので省略する。

【0238】

なお、ステップ S 3 3 5 において処理を終了し、HD 2 0 にライセンスを残すことも可能である。この場合、図 1 8 および図 1 9 に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

【0239】

なお、図 2 1 ～図 2 3 のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップ S 3 0 1 ～S 3 4 4 およびステップ S 3 4 7 ～S 3 7 1 のいずれかのステップにおいて処理が中断した場合には、再び図 2 1 ～図 2 3 に示されるフローチャートに従って再書込処理を行なうことができる。一方、ステップ S 3 2 5 ～S 3 4 6 のいずれかのステップにおいて処理が中断した場合には、図 1 8 および図 1 9 のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

【0240】

このようにして、端末装置 1 0 に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先の HD 2 1 から受取ったクラス証明書 C m 1 が有効であることを確認し、クラス証明書 C m 1 に含まれて送信されたクラス公開鍵 K P c m 1 によってライセンスの複製・移動が行なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンスの複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

。

【0241】

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるHD21における複製・移動セッションの対象となったライセンスLICに対する受信ログを送信側のデータ記憶装置であるHD20へ送信し、HD20において、自身のログメモリ253に格納されるログの内容と、そのログに記憶される格納LBAによって特定されるセキュアデータ記憶部250の領域に記憶されるライセンスLICとを比較し、さらに有効フラグ領域252に記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、2つのデータ記憶装置HD20およびHD21に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

【0242】

このように、本発明は、複製・移動セッションの中断によるライセンスLICの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

【0243】

なお、図18～図23におけるHD21の処理ステップS202, 203, S214, S215, S217～S220, S241～S243, S245～S251, S309, S310, S312～S322, S337～S340, S361～S363, S365～S371は、図9、図10および図13～図15におけるHD20の処理ステップS2, S3, S16, S17, S19～S22, S33～S35, S37～S43, S109, S110, S112～S122, S136～S139, S150～S152, S154～S160とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるHD21の処理とライセンスの配信処理時におけるHD20の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（HD20, HD21）においてライセンスを

書込むためのデータ記憶装置における処理である。

【0244】

[再生許諾]

再び図5を参照して、コンテンツデータを再生する再生回路150を備えた端末装置10にデータ記憶装置としてのHD20が装着され、コンテンツデータの再生許諾は、HD20から端末装置10内の再生回路150に対して行なわれる。

【0245】

図24は、端末装置10のユーザが端末装置10から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置10に装着されたHD20から端末装置10内の再生回路150へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

【0246】

図24を参照して、端末装置10のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置10のコントローラ108は、バスBS2を介して再生回路150へクラス証明書の出力要求を出力する（ステップS401）。再生回路150において、認証データ保持部1502は、バスBS2からクラス証明書の出力要求を受けると（ステップS402）、保持しているクラス証明書 $Cp3 = KPcp3 // Icp3 // E(Ka, H(KPcp3 // Icp3))$ をバスBS2へ出力する（ステップS403）。

【0247】

コントローラ108は、バスBS2からクラス証明書 $Cp3$ を受理すると（ステップS404）、受理したクラス証明書 $Cp3$ をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS405）。

【0248】

HD20では、端末装置10からクラス証明書 $Cp3$ を受理すると（ステップS406）、受理したクラス証明書 $Cp3$ が正当なクラス証明書であるか否かを検証する（ステップS407）。検証処理は、複製・移動セッションにおけるステップS207において説明したのと同様の方法で行なわれ、説明は省略する。

【0249】

ステップS407において、クラス証明書Cp3が正当な証明書であると判断された場合、コントローラ214は、クラス証明書Cp3を承認し、クラス証明書Cp3に含まれるクラス公開鍵KPcp3を受理する（ステップS408）。そして、次の処理（ステップS409）へ移行する。コントローラ214は、正当なクラス証明書でない場合には、クラス証明書Cp3を非承認とし、クラス証明書Cp3を受理せずにエラー通知を端末装置10へ出力し（ステップS435）、端末装置10においてエラー通知が受理されると（ステップS436）、再生許諾セッションが終了する。

【0250】

ステップS408においてクラス公開鍵KPcp3が受理されると、HD20のセッション鍵発生部226は、セッション鍵Ks1dを生成する（ステップS409）。セッション鍵Ks1dは、受理されたクラス公開鍵KPcp3によって、暗号処理部222において暗号化され、暗号化データE（KPcp3, Ks1d）が生成される（ステップS410）。

【0251】

そして、コントローラ214は、暗号処理部222からバスBS3を介して暗号化データE（KPcp3, Ks1d）を受けると、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS411）。

【0252】

端末装置10において、HDインターフェース部110およびバスBS2を介してコントローラ108が暗号データE（KPcp3, Ks1d）を受理すると（ステップS412）、コントローラ108は、受理した暗号化データE（KPcp3, Ks1d）をバスBS2を介して再生回路150へ出力する（ステップS413）。再生回路150の復号処理部1506は、バスBS2から暗号化データE（KPcp3, Ks1d）を受理すると（ステップS414）、Kcp保持部1504に保持される再生回路150に固有なクラス秘密鍵Kcp3によって復号処理することによりセッション鍵Ks1dを復号し、セッション鍵Ks1

dが受理される（ステップS415）。

【0253】

セッション鍵Ks1dが受理されると、セッション鍵発生部1508は、セッション鍵Ks2dを生成し（ステップS416）、生成したセッション鍵Ks2dを暗号処理部1510に与える。暗号処理部1510は、復号処理部1506から受けるセッション鍵Ks1dをセッション鍵Ks2dにより暗号化し、暗号化データE（Ks1d, Ks2d）を生成する（ステップS417）。そして、暗号処理部1510は、暗号化データE（Ks1d, Ks2d）をバスBS2へ出力する（ステップS418）。

【0254】

コントローラ108は、バスBS2から暗号化データE（Ks1d, Ks2d）を受理し（ステップS419）、受理したデータをバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS420）。

【0255】

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE（Ks1d, Ks2d）を受理すると（ステップS421）、受理したデータをバスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks1dを用いてバスBS3に出力された暗号化データE（Ks1d, Ks2d）を復号し、HD20においてセッション鍵Ks2dが受理される（ステップS422）。そして、コントローラ214は、セッション鍵Ks2dが受理されると、その旨の通知をATAインターフェース部212および端子210を介して端末装置10へ出力する。

【0256】

端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介してHD20においてセッション鍵Ks2dが受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンスLICが格納されているセキュアデータ記憶部250のLBAをバスBS2およびHDインターフェース部110を介してHD20へ出力する。

【0257】

HD20のコントローラ214は、端子210およびATAインターフェース部212を介して対象のライセンスLICが格納されているLBAを受理すると（ステップS424）、そのLBAに格納されるライセンスLICに対応する有効フラグ領域252のフラグが“有効”であるか“無効”であるかを確認する（ステップS425）。

【0258】

コントローラ214は、有効フラグ領域252のフラグが“有効”であると、受理したLBAに基づいて、対象のライセンスLICをセキュアデータ記憶部250から取得する（ステップS426）。そして、コントローラ214は、取得したライセンスLICに含まれる制御情報ACの内容を確認する（ステップS427）。コントローラ214は、制御情報ACにおいて利用回数が指定されているときは、制御情報ACの利用回数を1増分し、次の処理（ステップS429）へ移行する。一方、コントローラ214は、制御情報ACにより再生制限がかけられていないときは、取得したライセンスLICに含まれるコンテンツ鍵KcをバスBS3へ出力する。

【0259】

暗号処理部224は、復号処理部228から受けるセッション鍵Ks2dによりバスBS3上に出力されたコンテンツ鍵Kcを暗号化して暗号化データE（Ks2d，Kc）を生成し（ステップS429）、生成したデータをバスBS3へ出力する。そして、コントローラ214は、バスBS3上に出力された暗号化データE（Ks2d，Kc）をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS430）。

【0260】

端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して暗号化データE（Ks2d，Kc）を受理すると（ステップS431）、受理したデータをバスBS2へ出力する（ステップS432）。

【0261】

再生回路150の復号処理部1512は、バスBS2から暗号化データE（K

s 2 d, K c) を受理すると (ステップ S 4 3 3)、セッション鍵発生部 1 5 0 8 から与えられるセッション鍵 K s 2 d を用いて暗号化データ E (K s 2 d, K c) を復号する。これにより、再生回路 1 5 0 においてコンテンツ鍵 K c が受理され (ステップ S 4 3 4)、一連の再生許諾セッションの処理が正常終了する。

【0262】

一方、ステップ S 4 2 5 において、有効フラグ領域 2 5 2 のフラグが “無効” であったとき、またはステップ S 4 2 7 において、制御情報 A C に含まれる内容が再生不可であったときは、コントローラ 2 1 4 は、端末装置 1 0 に対してエラー通知を出力し (ステップ S 4 3 5)、端末装置 1 0 においてエラー通知が受理されると (ステップ S 4 3 6)、再生許諾セッションが終了する。

【0263】

このようにして、データ記憶装置である H D 2 0 から端末装置 1 0 に備えられる再生回路 1 5 0 への再生許諾に関しても、再生回路 1 5 0 が正規のクラス証明書 C p 3 を保持していること、およびクラス証明書 C p 3 に含まれて送信されたクラス公開鍵 K P c p 3 が有効であることを確認した上でコンテンツ鍵 K c が再生回路 1 5 0 へ送信され、不正なコンテンツデータの再生を禁止することができる。

【0264】

なお、フローチャートにおいて図示しないが、再生回路 1 5 0 は、コンテンツの再生許諾がなされ、コンテンツ鍵 K c を受理すると、H D 2 0 から出力された暗号化コンテンツデータ E (K c, D c) を復号処理部 1 5 1 4 において復号し、再生部 1 5 1 6 において復号処理部により復号されたデータ D c が再生され、D A 変換部 1 5 1 8 によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子 1 5 2 0 へ再生信号が出力される。

【0265】

このように、H D 2 0 では、ライセンスの漏洩が無いように安全に保護し、記憶、入出力の管理を行なうために、

(1) 他の装置 (ライセンス提供装置または他の H D) からライセンスの提供を

受けて格納する書込処理（図 9 および図 10 における HD 20 および図 21～図 23 における HD 21 の処理）

（2）書込処理の中断から、書込処理を再開する再書込処理（図 13～図 15 に

おける HD および図 21～図 23 における HD 21 の処理）

（3）他の HD に対してライセンスを移動または複製する提供処理（図 16～図

18 における HD 20 の処理）

（4）提供処理の中断から、移動複製処理を再開する再提供処理（ライセンスの

提供元としての再書込処理、図 21～図 23 における HD 20 の処理）

（5）暗号化コンテンツデータを復号することを目的として再生回路に対してコ

ンテンツ鍵 K_c を提供する再生許諾処理（図 24 における HD 20 の処理）

の 5 つの処理を、暗号技術によって実現している。

【0266】

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

【0267】

〔実施の形態 2〕

実施の形態 1 においては、HD 20 は、図 13～図 15 のフローチャートに示される再書込処理および図 21～図 23 のフローチャートに示される再提供処理において、再書込／提供処理を開始するにあたって、処理の可否を判断するために、再書込／提供処理の対象となるライセンスに対する直前のログを検索する。そして、対応したログが検索された場合、検索したログをログメモリ 253 のバンク n に複製して、以後の処理においてはバンク n に格納されたログを処理の手

順に従って更新していくものとして説明した。

【0268】

しかし、再書込処理においては、複製したログはライセンスの提供側に対して直前の処理に対するログとして出力した後、図14のステップS137において、その内容が書換えられてしまう。ログの複製は、古いログが格納されたバンクから順に新たなログの格納バンクに向けて循環的に使用していくログメモリ253の特性に由来するものであり、再書込処理の初期における中断（図14のステップS136以前）においても、再書込処理に対応するログが、より長くログメモリ253に保持されることを目的としている。

【0269】

したがって、十分に大きなログメモリ253を備えたHDにおいては、再書込処理における検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接出力するように構成することも可能である。この場合、ステータスST2の変更（ステップS115, S116, S117）は、当該バンクのログに対して行なわれ、出力するためのログの取得（ステップS118）は、当該バンクから行なわれることとなる。

【0270】

また、ログの複写がなされないため、再書込処理に対応するログを格納するためのバンクは、図14のステップS137において確保される。したがって、ステップS137は、「ログメモリの最も古いログを格納しているバンクnaに新たなログを格納」と変更される。

【0271】

さらに、HD21も同様に処理を変更することが可能である。その他の全ての処理は、実施の形態1と同じである。なお、この処理の変更によってライセンスの安全性は何ら変化することはなく、実施の形態1と同様の効果を得ることができる。

【0272】

〔実施の形態3〕

ライセンスの再書込処理と同様に、ライセンスの再提供処理において、検索さ

れたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接読出し、再提供の可否を判定することも可能である。図21のステップS301aにおいて複製を行なうことなく、図21のステップS302および図22のステップS329, S331, S332において検索されたログが格納されていたバンクから直接ログを取得するように処理を変更すればよい。その他の全ての処理は、実施の形態1と同じである。

【0273】

この処理の変更によってライセンスの安全性は、何ら変化することはなく、実施の形態1と同様の効果を得ることができる。また、実施の形態2と組合わせることも可能である。

【0274】

[実施の形態4]

HD20の実装における処理を軽減するためには、通常の手入処理および再手入処理は、より共通していることが望ましい。そこで、実施の形態1における「セッション鍵要求」移行のHD20における処理、すなわち、通常の手入処理（図9のステップS19～S22、図10のステップS33～S35, S38～S43）と再手入処理（図14のステップS136～S139、図15のステップS150～S152, S154～S160）を共通とする。この場合、図9のステップS20と図14のステップS137とを同一処理とすることで容易に実現できる。

【0275】

この場合、ステップS137をステップS20と同一処理とし、“ログメモリの最も古いログを格納しているバンクnbに新たなログを格納”とする。また、詳細な処理は、図11および図12のフローチャートに従い、変数nを変数nbと読替えればよい。また、変数nを変数nbと読替えるのは、図13および図14のステップS137までの処理における変数nと区別するためである。これに伴って、図14および図15のステップS137以降のステップS154, S155, S159におけるバンクnを全てバンクnbと読替える。

【0276】

同様に、移動複製セッションでは、図 21～図 23 のフローチャートに示されるステップ S 3 4 2 以降の処理と、図 16～図 18 のフローチャートに示されるステップ S 2 2 2 以降の処理との違いが、ログの記録の違い（図 23 のステップ S 3 4 5 と図 18 のステップ S 2 2 5 との違い）のみである。図 23 のステップ S 3 4 5 の処理を図 18 のステップ S 2 2 5 と同一の処理とすることによって H D 2 0 の実装を容易にすることができる。この場合、ステップ S 3 4 5 をステップ S 2 0 と同一処理とし、“ログメモリの最も古いログを格納しているバンク n b に新たなログを格納”とする。また、詳細な処理は、図 20 および図 12 のフローチャートに従い、変数 n を変数 n b と読替えればよい。また、変数 n を変数 n b と読替えるのは、図 21 および図 22 のステップ S 2 4 5 までの処理における変数 n と区別するためである。これに伴って、図 23 のステップ S 3 4 5 以降のステップ S 3 4 8, S 5 7 におけるバンク n を全てバンク n b と読替える。

【0277】

その他の全ての処理は、実施の形態 1 と同一である。また、処理の変更によってライセンスの安全性は何ら変化することなく、実施の形態 1 と同様な効果を得ることができる。さらに、H D 2 1 も同様に処理を変更することが可能である。

【0278】

このように、通常書込処理および再書込処理の共通化によって、実施の形態 1 と同様なライセンスの安全な管理を実現した上で実装する処理量の軽減を図ることができる。

【0279】

〔実施の形態 5〕

ログの記録開始タイミングを明確にするために、全ての処理において H D 外部からライセンス I D (L I D) を受理することによって、ログメモリ 2 5 3 からバンクを 1 つ確保し、当該処理に対するログを記録するように変更した実施の形態 5 について説明する。

【0280】

まず、実施の形態 5 におけるライセンスの配信動作について説明する。

実施の形態 5 においては、ライセンス提供措置 4 0 から H D 2 0 へのライセン

スの配信は、図 25 および図 26 に示すフローチャートに従って行なわれる。図 25 および図 26 に示すフローチャートは、図 9 および図 10 に示すフローチャートのステップ S 16 とステップ S 17 との間にステップ S 16 a を挿入し、ステップ S 20 をステップ S 20 1 a に代えたものであり、その他は図 9 および図 10 に示すフローチャートと同じである。

【0281】

ステップ S 16 a の詳細な動作は、図 27 に示すフローチャートに従って行なわれる。図 27 を参照して、HD 20 にコントローラ 214 は、ステップ S 16 の後、最新のログが格納されているバンク n-1 を特定し、バンク n に格納されている管理番号 m を取得する（ステップ S 16 b）。そして、このステップ S 16 b の詳細な動作は、図 12 に示すフローチャートに従って行なわれる。

【0282】

コントローラ 214 は、ステップ S 16 b の後、管理番号 m+1、およびステップ S 16 で受理したライセンス ID (LID) をバンク n に格納し、バンク n に格納されたログの ST 1 領域 2544 を“受信待”に設定する（ステップ S 16 c）。これにより、図 25 に示すステップ S 16 a の動作が終了する。

【0283】

また、コントローラ 214 は、ステップ S 19 の後、ログメモリ 253 のバンク n に格納されたログの K s 2 x 領域 2543 に、ステップ S 19 で受理したセッション鍵 K s 2 a を記録する（ステップ S 20 1 a）。

【0284】

その他は、実施の形態 1 において説明したとおりである。

〔配信における再書込〕

実施の形態 5 におけるライセンスの配信が途中で中断した場合のライセンスの再書込の動作は、図 13～図 15 に示すフローチャートに従って行なわれる。その詳細な動作は実施の形態 1 において説明したとおりである。

【0285】

〔移動／複製〕

図 28 および図 29 は、図 17 に示すライセンスの複製・移動が可能なシステ

ムにおいて、端末装置 10 のユーザが端末装置 10 から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置 10 を介して端末装置 10 に装着された HD 20 から HD 21 へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための実施の形態 5 における第 1 および第 2 のフローチャートである。

【0286】

図 28 および図 29 に示すフローチャートは、図 18 および図 19 に示すフローチャートのステップ S 207 とステップ S 209 との間にステップ S 208 を挿入し、ステップ S 214 とステップ S 215 との間にステップ S 214a を挿入し、ステップ S 218 をステップ S 218a に代え、ステップ S 225 をステップ S 225a に代えたものであり、その他は図 18 および図 19 に示すフローチャートと同じである。

【0287】

図 28 を参照して、HD 20 のコントローラ 214 は、ステップ S 207 において HD 21 からの証明書 Cm1 を承認したとき、ログメモリ 253 のうち最も古いログが格納されたバンク n に新たなログを格納する（ステップ S 208）。このステップ S 208 の詳細な動作は、図 30 に示すフローチャートに従って行なわれる。

【0288】

図 30 を参照して、ステップ S 208 は、HD 20 においてログメモリ 253 の最新ログが記録されたバンク n-1 を特定し、かつ、バンク n-1 に格納された管理番号 m を取得するステップ S 208a と、バンク n に、管理番号 m+1、ライセンス ID (LID)、およびクラス公開鍵 K P c m y を格納し、かつ、S T 1 領域 2544 のステータス S T 1 を“送信待”に設定するステップ S 208b とから成る。そして、ステップ S 208a の詳細な動作は、図 12 に示すフローチャートに従って行なわれる。したがって、コントローラ 214 は、図 12 および図 30 に示すフローチャートに従って、ステップ S 206 において受理したライセンス ID (LID) と HD 21 のクラス公開鍵 K P c m 1 と、“送信待”に設定されたステータス S T 1 とを記録した新たなログをバンク n に格納する。

【0289】

また、HD21のコントローラ214は、ステップS214の後、最も古いログが格納されたバンクnaに新たなログを格納する（ステップS214a）。このステップS214aの詳細な動作は、上述した図12および図27に示すフローチャートに従って行なわれる。ただし、変数nは、変数naに読替える。

【0290】

したがって、HD21のコントローラ214は、図12および図27に示すフローチャートに従って、ステップS214において受理したライセンスID（LID）と、“受信待”に設定されたステータスST1とを記録した新たなログを、ログメモリ254の中で最も古いログが格納されていたバンクnaに格納する（ステップS214a）。

【0291】

さらに、HD21のコントローラ214は、ステップS217の後、ログメモリ253のバンクnaにステップS217において生成されたセッション鍵Ks2aを格納する（ステップS218a）。

【0292】

さらに、HD20のコントローラ214は、ステップS224の後、ログメモリ253のバンクnに、ステップS224で受理したセッション鍵Ks2aを格納する（ステップS225a）。

【0293】

その他は、実施の形態1において説明したとおりである。

[移動／複製における再書込]

実施の形態5におけるHD21からHD20へのライセンスの移動・複製セッションが途中で中断した場合のライセンスの再書込動作は、図21～図23に示すフローチャートに従って行なわれる。したがって、その詳細な動作は実施の形態1で説明したとおりである。

【0294】

このように、実施の形態5では、実施の形態1と同様に安全なライセンスの再書込／提供処理を実現し、かつ、それぞれの処理におけるログの発生タイミング

を明確にするとともに、実施の形態3と同様に、通常書込／再書込処理の共通化によって実装する処理量の軽減を図ることができる。なお、HD21も同様に処理を変更することが可能である。

【0295】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおいて使用される暗号通信に用いられる鍵、情報等の特性を示す図である。

【図4】 図1に示すライセンス提供装置の構成を示す概略ブロック図である。

【図5】 図1に示す端末装置の構成を示す概略ブロック図である。

【図6】 図1に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

【図7】 図6に示すハードディスクにおけるセキュアデータ記憶部の構成を示す図である。

【図8】 図6に示すハードディスクにおけるノーマルデータ記憶部の構成を示す図である。

【図9】 図1に示すデータ配信システムにおける配信処理を説明するための実施の形態1における第1のフローチャートである。

【図10】 図1に示すデータ配信システムにおける配信処理を説明するための実施の形態1における第2のフローチャートである。

【図11】 図9に示すステップS20の詳細な動作を説明するためのフローチャートである。

【図 12】 図 11 に示すステップ S 20 a の詳細な動作を説明するためのフローチャートである。

【図 13】 図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 1 のフローチャートである。

【図 14】 図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 2 のフローチャートである。

【図 15】 図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態 1 における第 3 のフローチャートである。

【図 16】 図 13 に示すステップ S 112 a の詳細な動作を説明するためのフローチャートである。

【図 17】 複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

【図 18】 図 17 に示すシステムにおける複製または移動処理を説明するための実施の形態 1 における第 1 のフローチャートである。

【図 19】 図 17 に示すシステムにおける複製または移動処理を説明するための実施の形態 1 における第 2 のフローチャートである。

【図 20】 図 18 に示すステップ S 218 の詳細な動作を説明するためのフローチャートである。

【図 21】 図 17 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 1 のフローチャートである。

【図 22】 図 17 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 2 のフローチャートである。

【図 23】 図 17 に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態 1 における第 3 のフローチャートである。

【図 24】 図 5 に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

【図 25】 図 1 に示すデータ配信システムにおける配信処理を説明するための実施の形態 5 における第 1 のフローチャートである。

【図 26】 図 1 に示すデータ配信システムにおける配信処理を説明するた

めの実施の形態5における第2のフローチャートである。

【図27】 図25に示すステップS16aの詳細な動作を説明するためのフローチャートである。

【図28】 図17に示すシステムにおける複製または移動処理を説明するための実施の形態5における第1のフローチャートである。

【図29】 図17に示すシステムにおける複製または移動処理を説明するための実施の形態5における第2のフローチャートである。

【図30】 図28に示すステップS208の詳細な動作を説明するためのフローチャートである。

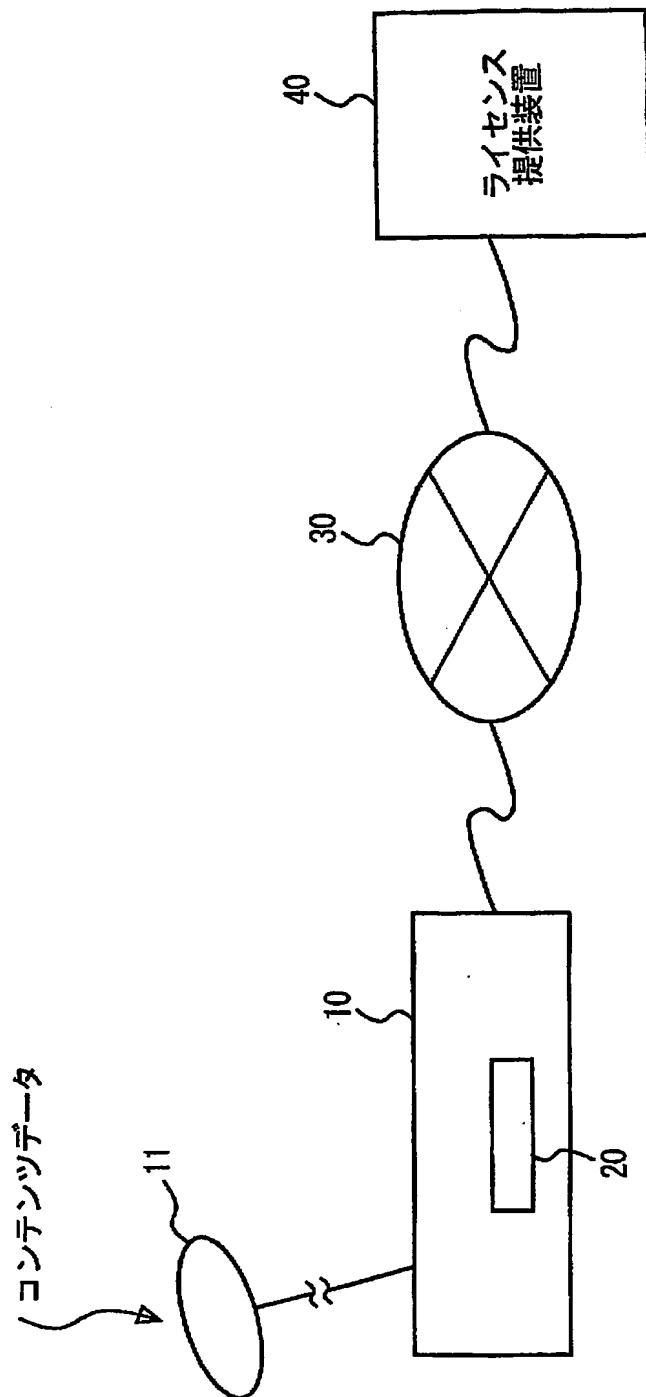
【符号の説明】

10 端末装置、11 アンテナ、20, 21 ハードディスクドライブ (HD)、30 ネットワーク、40 ライセンス提供装置、102 アンテナ、104 受信部、106 モデム、108 コントローラ、110 HDインターフェース部、150 再生回路、202, 1502 認証データ保持部、204 Kcm保持部、206 Kom保持部、208 KPom保持部、210, 1520 端子、212 ATAインターフェース部、214 コントローラ、216, 228, 230, 422, 1506, 1512, 1514 復号処理部、218, 416 KP a保持部、220, 418 認証部、222, 224, 232, 420, 424, 426, 1510 暗号処理部、226, 414, 1508 セッション鍵発生部、250 セキュアデータ記憶部、251 ライセンス領域、252 有効フラグ領域、253 ログメモリ、260, 262 切替スイッチ、270 ノーマルデータ記憶部、402 コンテンツDB、404 ログDB、410 データ処理部、412 配信制御部、450 通信装置、1504 Kcp保持部、1516 再生部、1518 DA変換部、2541 管理番号領域、2542 ライセンスID領域、2543 Ks2x領域、2544 ST1領域、2545 ST2領域、2546 KPcmx領域、2547 LBA領域、2701 磁気記録媒体、2702 モータ、2703 サーボ制御部、2704 シーク制御部、2705 記録再生処理部、BS1～BS3 バス。

【書類名】

図面

【図 1】



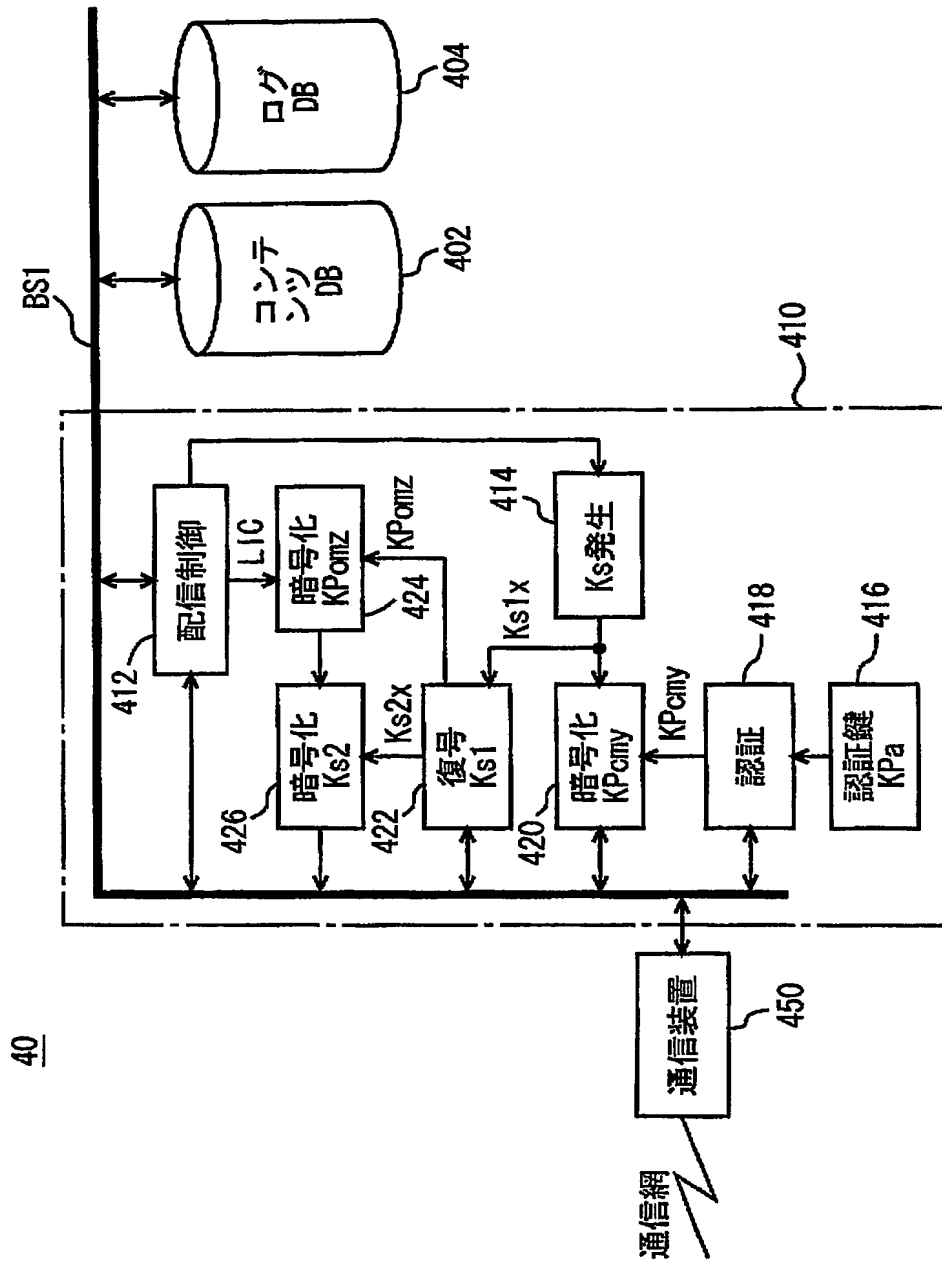
【図 2】

記号	名称	属性	特性
Dc	データ	データ固有	例: 音楽データ、朗読データ、教材データ、画像データ Kcにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号/復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

【図 3】

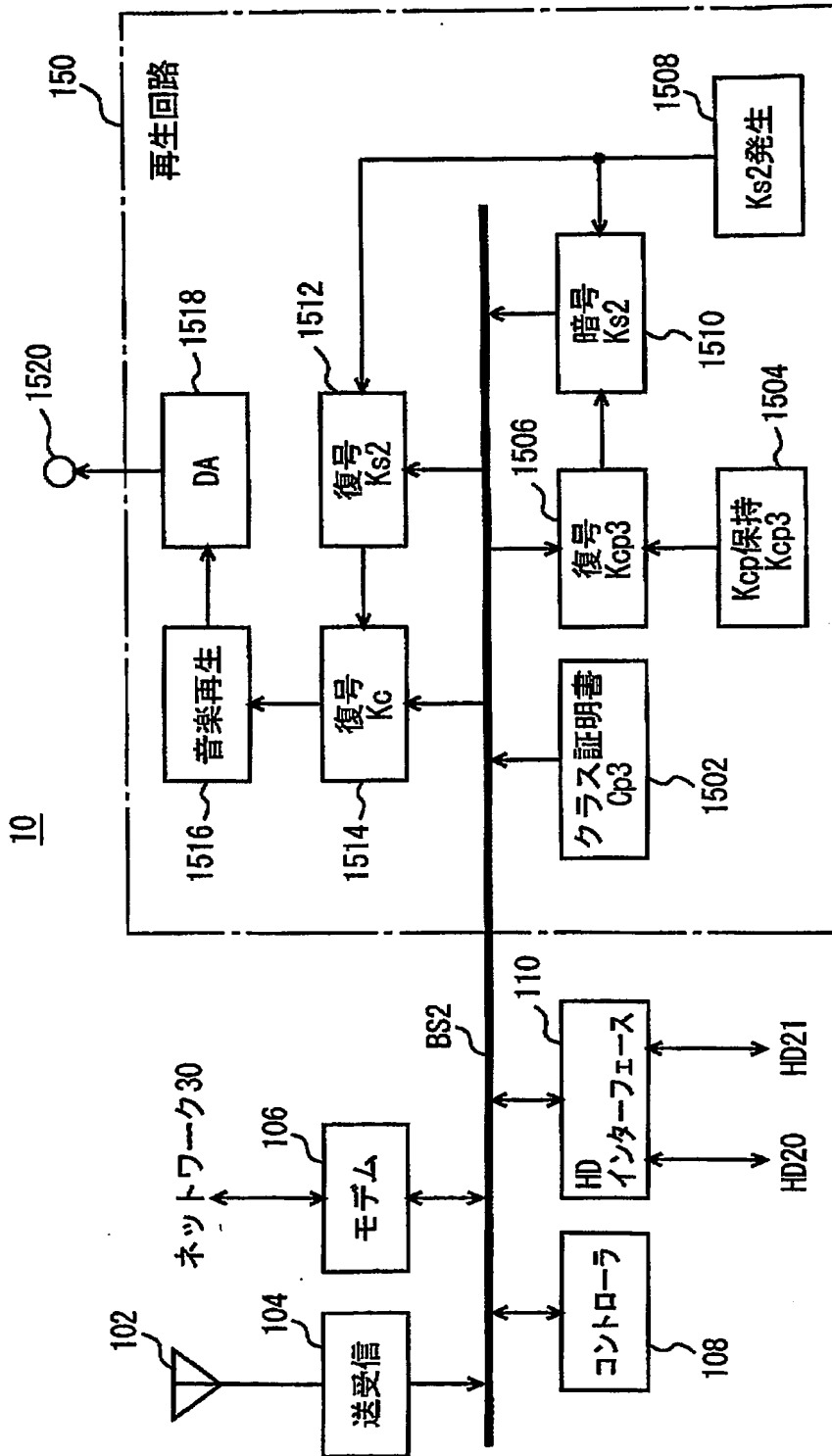
記号	名称	特性
ライセンサ提供装置	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンサ提供側にて運用される
	セッション鍵	ライセンサの配信ごとに生成される一時鍵 共通鍵
	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵 認証局にて運用される
データ記録装置 (ハードディスク)	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンサ提供側にて運用される
	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「Y」はクラスを識別するための識別子
	クラス秘密鍵	クラス公開鍵(KPomy)にて暗号化されたデータを復号する非対称な復号鍵
	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	クラス証明書	Cmy=K(Pomy//lcmv//E(Ka,H(KPomy//lcmv))) 認証鍵(KPal)によってその正当性が確認できる
	個別公開鍵	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 「Z」はデータ記録装置を識別するための識別子
	個別秘密鍵	個別公開鍵(KPomz)にて暗号化されたデータを復号する非対称な復号鍵
	セッション鍵	ライセンサの授受ごとにライセンサ提供側で生成される一時鍵 共通鍵
	セッション鍵	ライセンサの授受ごとにライセンサ受理側で生成される一時鍵 共通鍵
	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「Y」はクラスを識別するための識別子
再生回路	クラス秘密鍵	クラス公開鍵(KPcpy)にて暗号化されたデータを復号する非対称な復号鍵
	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	クラス証明書	Cpy=K(Pcpy//lcpy//E(Ka,H(KPcpy//lcpy))) 認証鍵(KPal)によってその正当性が確認できる
	セッション鍵	ライセンサの授受ごとにライセンサ受理側で生成される一時鍵 共通鍵
	セッション鍵	ライセンサの授受ごとにライセンサ受理側で生成される一時鍵 共通鍵

【図 4】

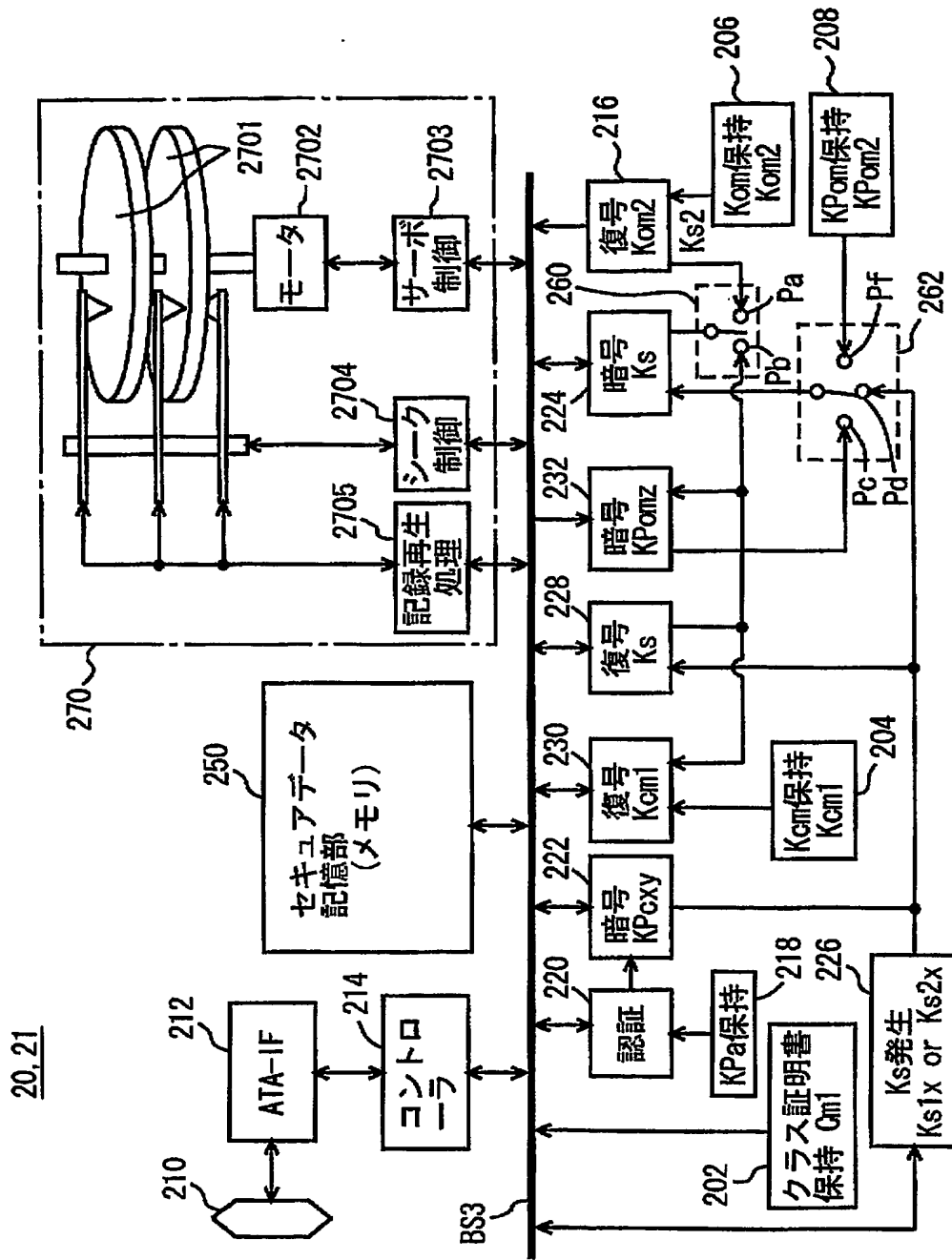


40

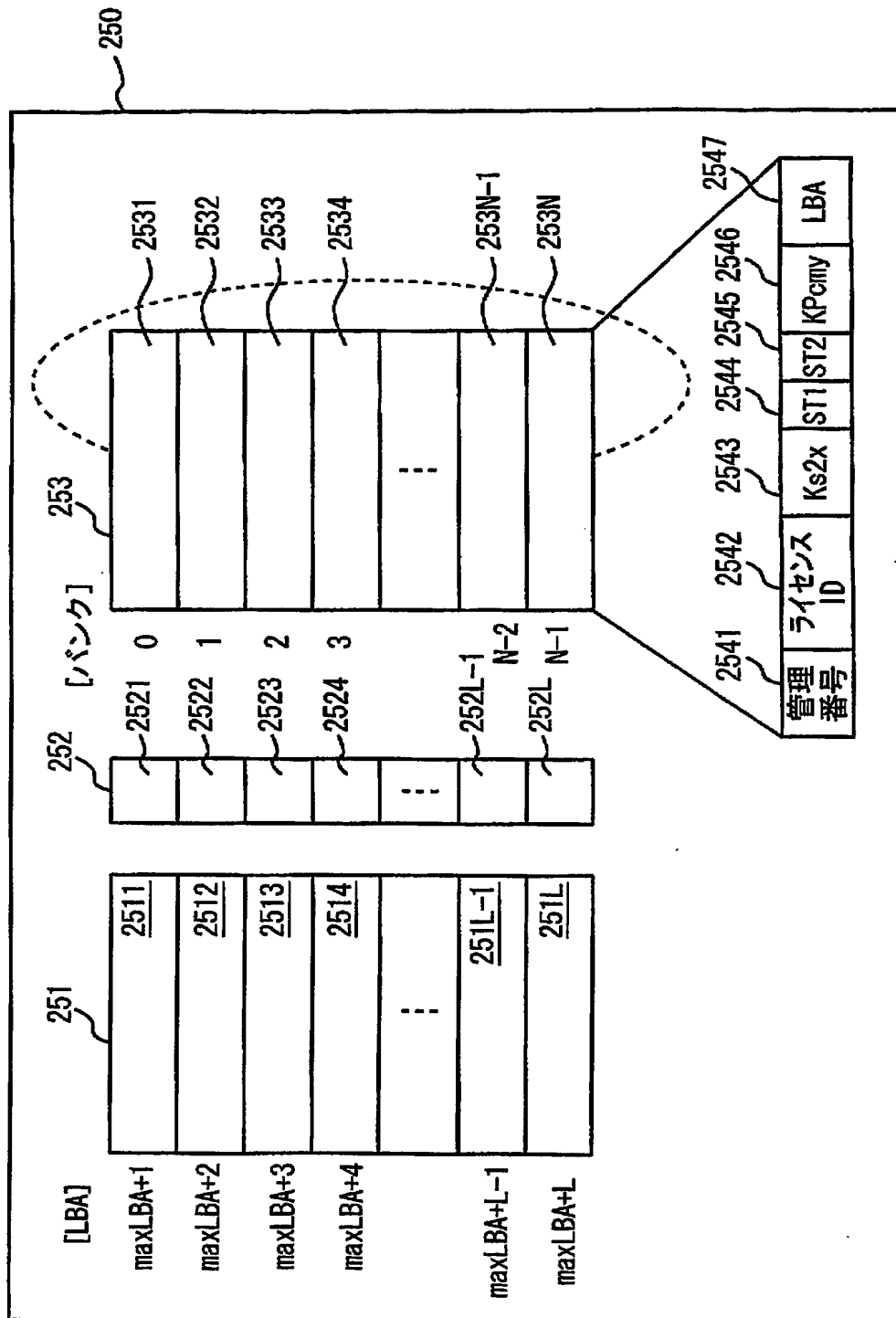
【図 5】



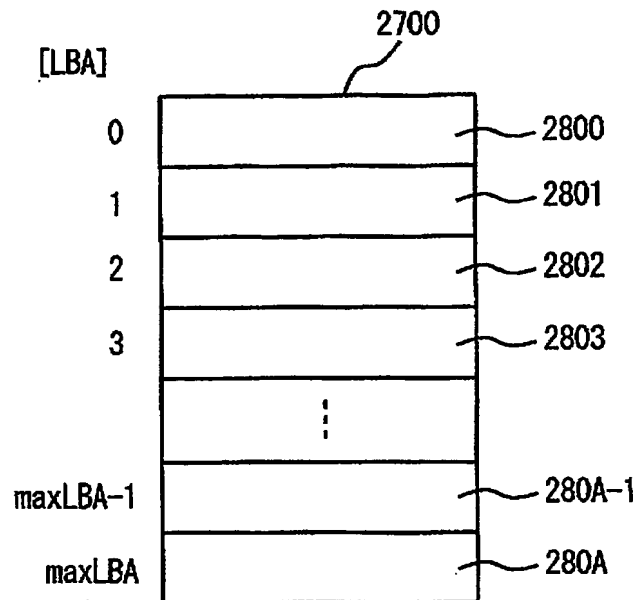
【図 6】



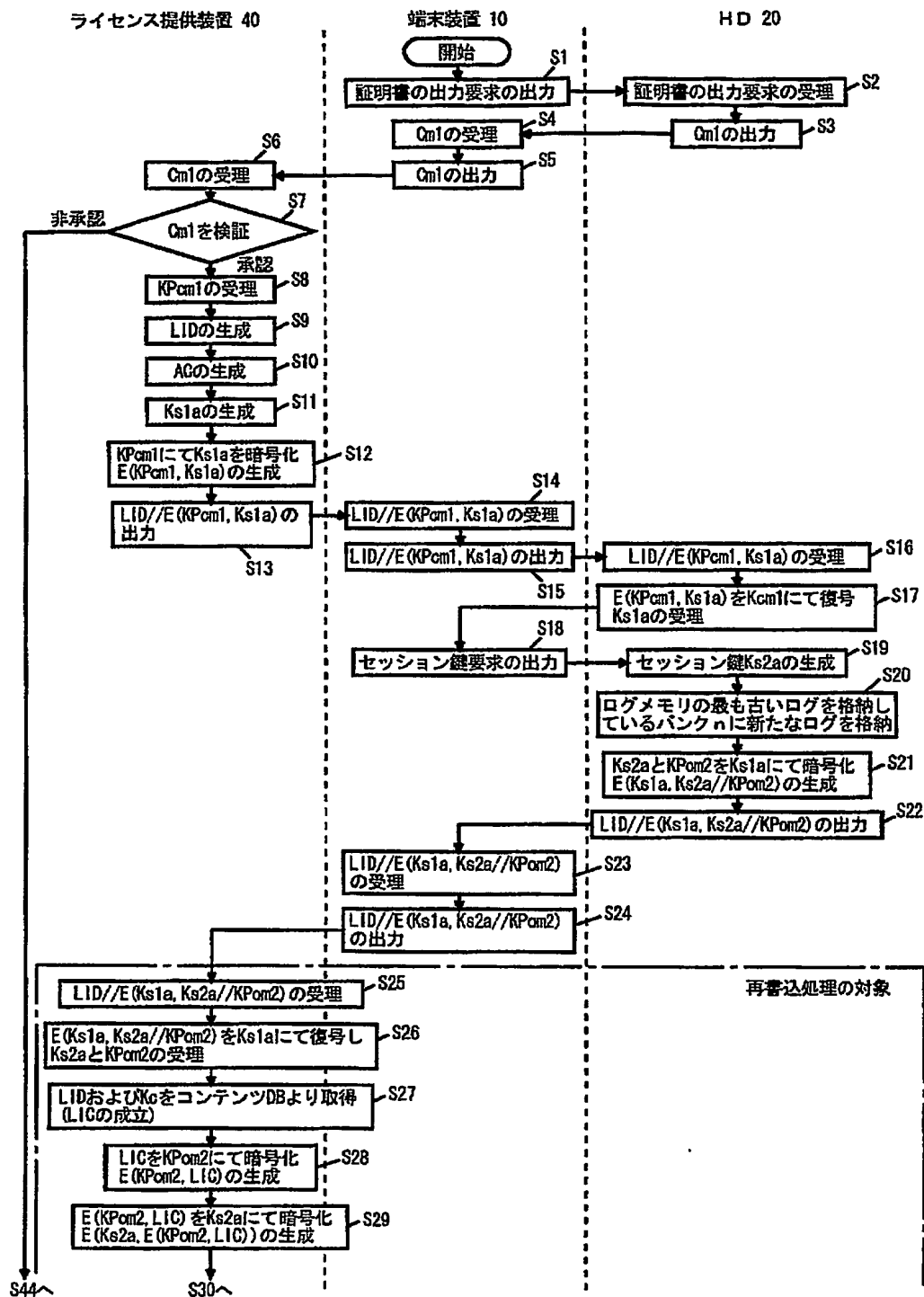
【図 7】



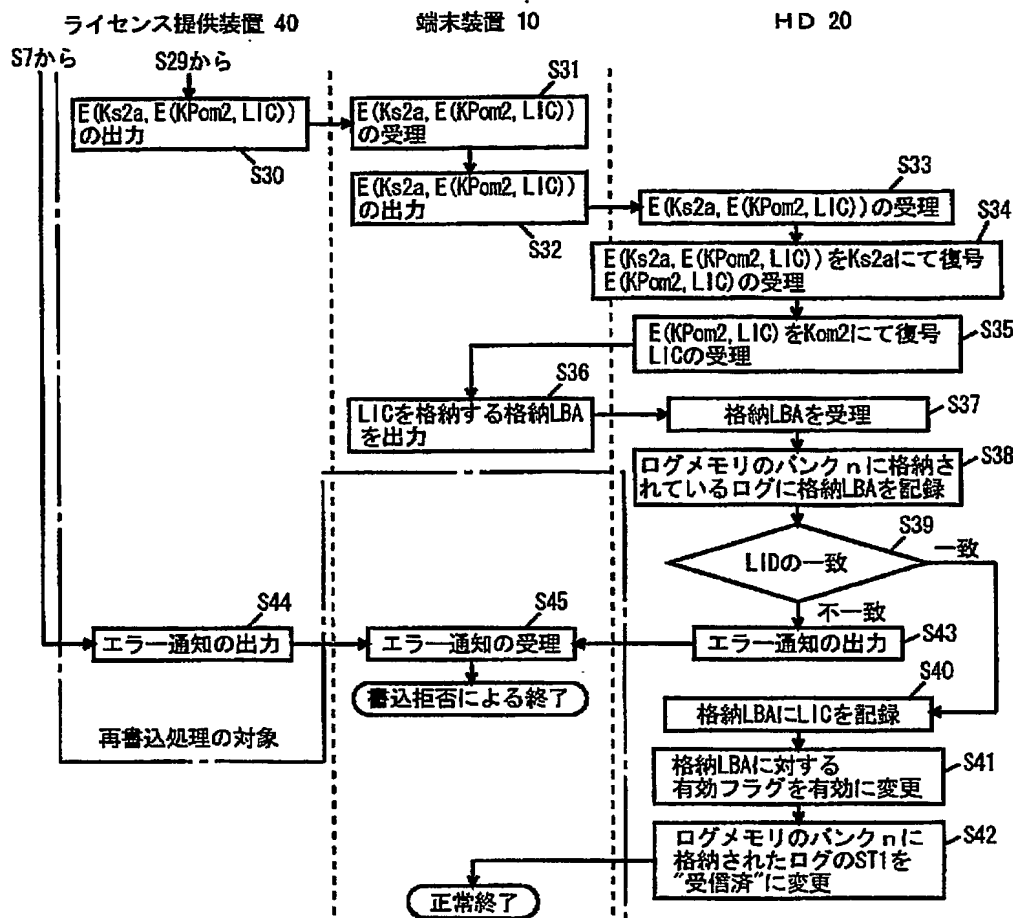
【図 8】



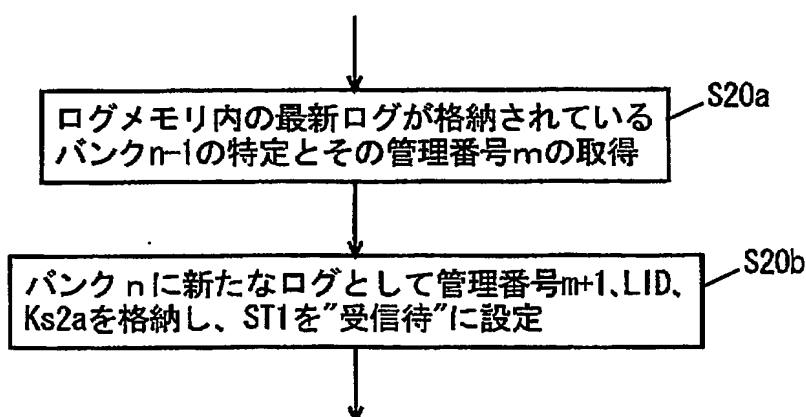
【図 9】



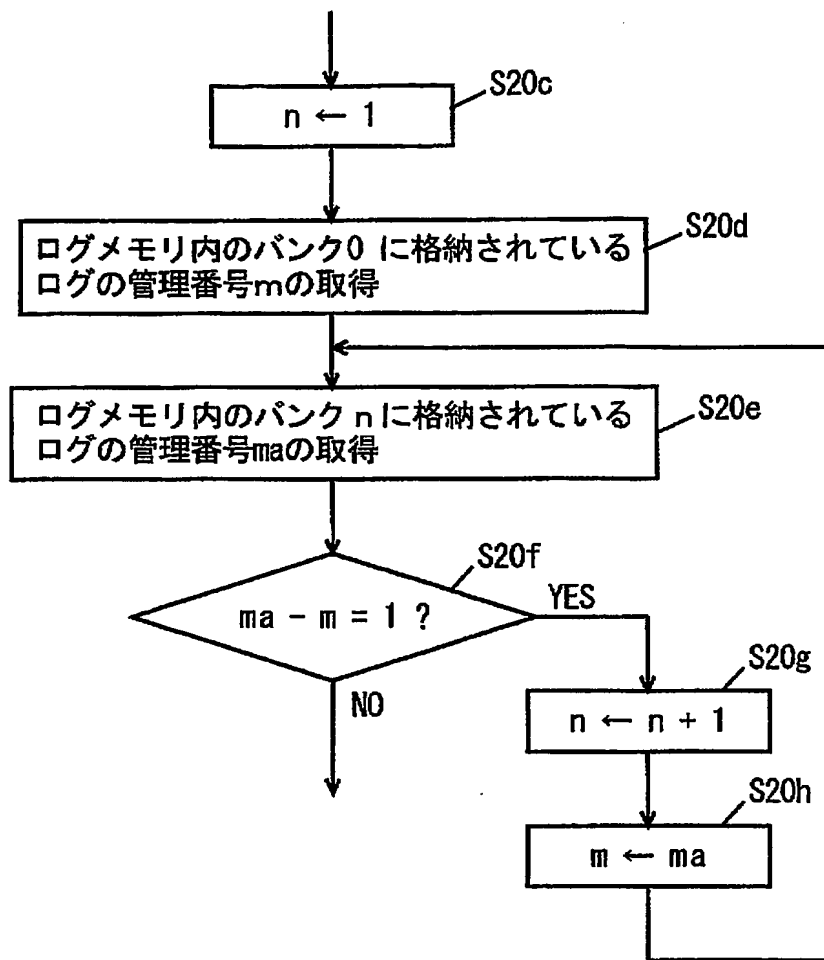
【图 10】



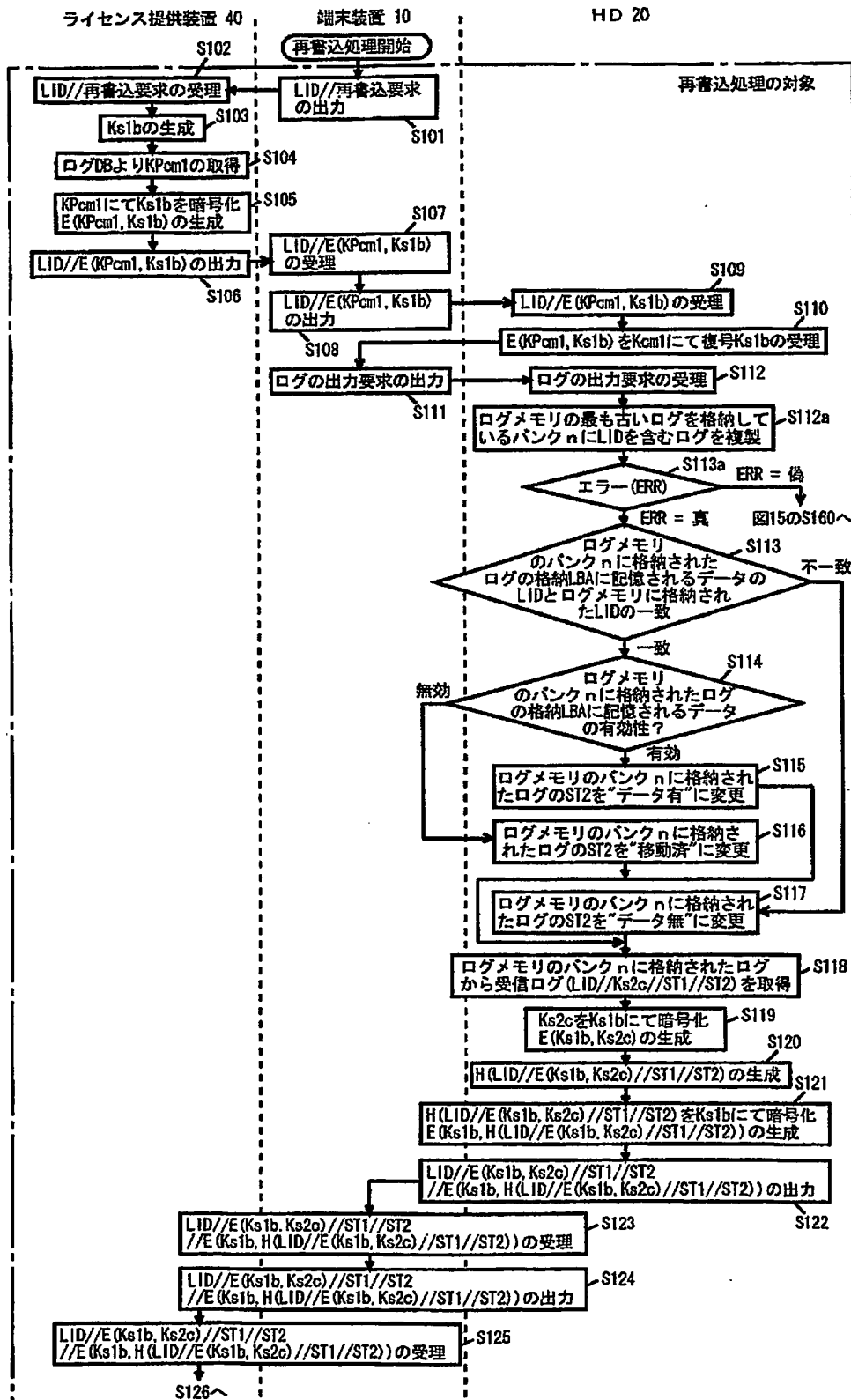
【图 1-1】



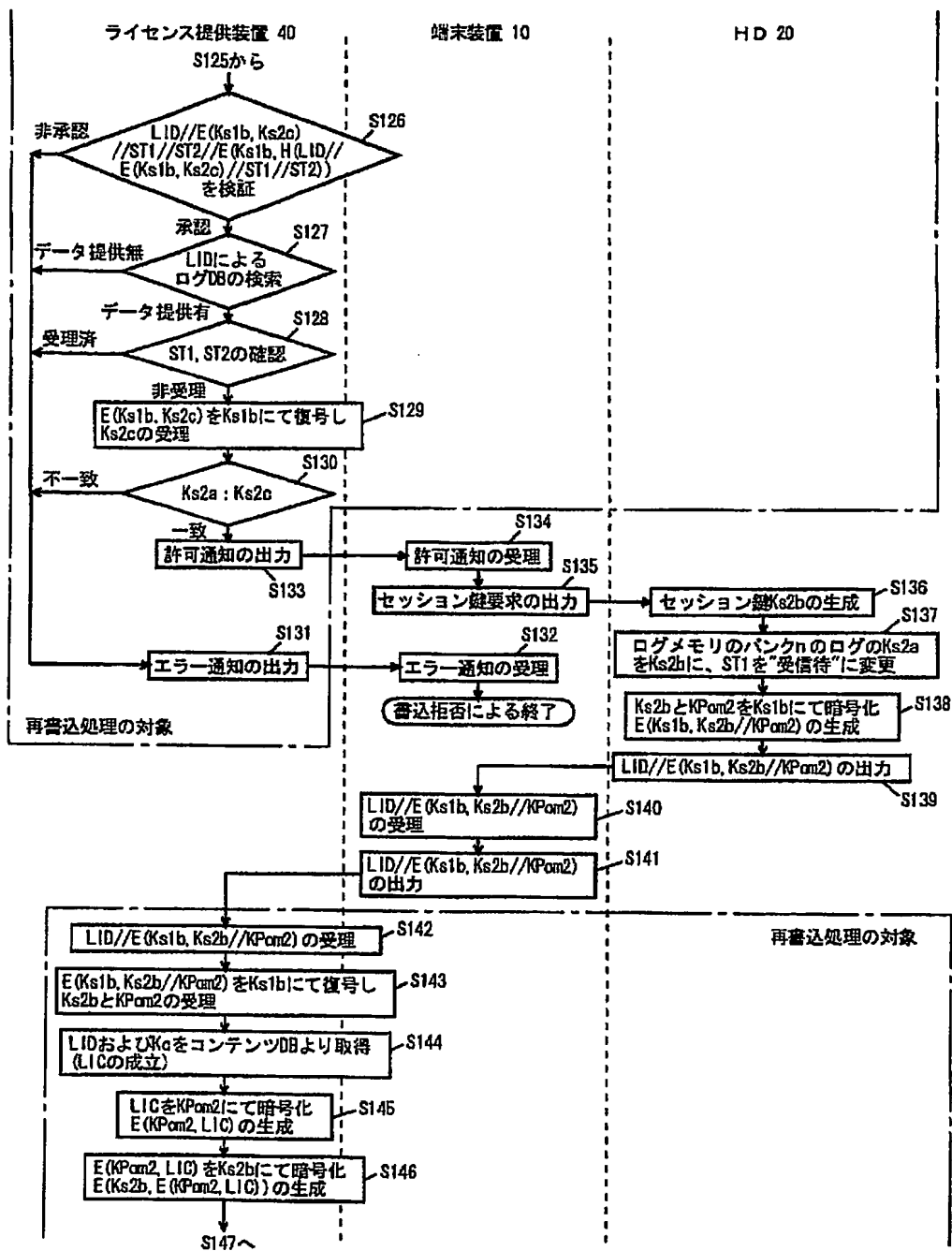
【図 12】



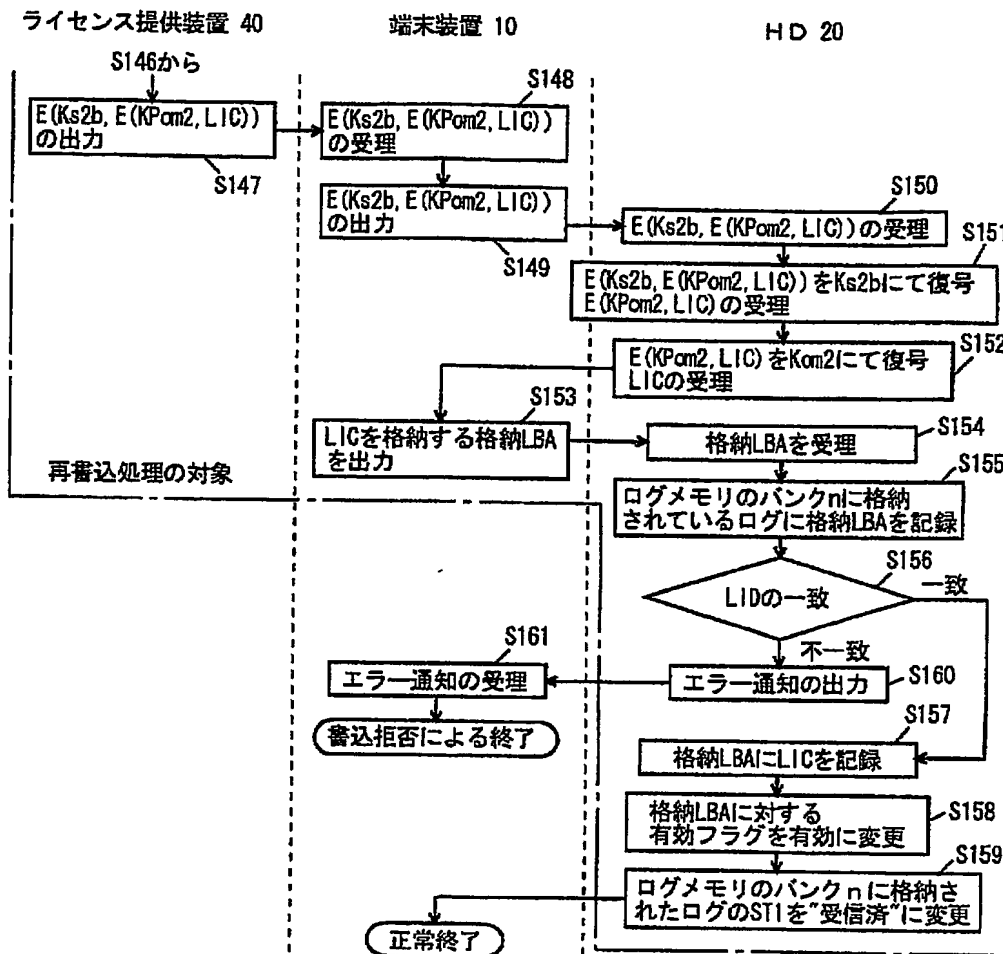
【図 13】



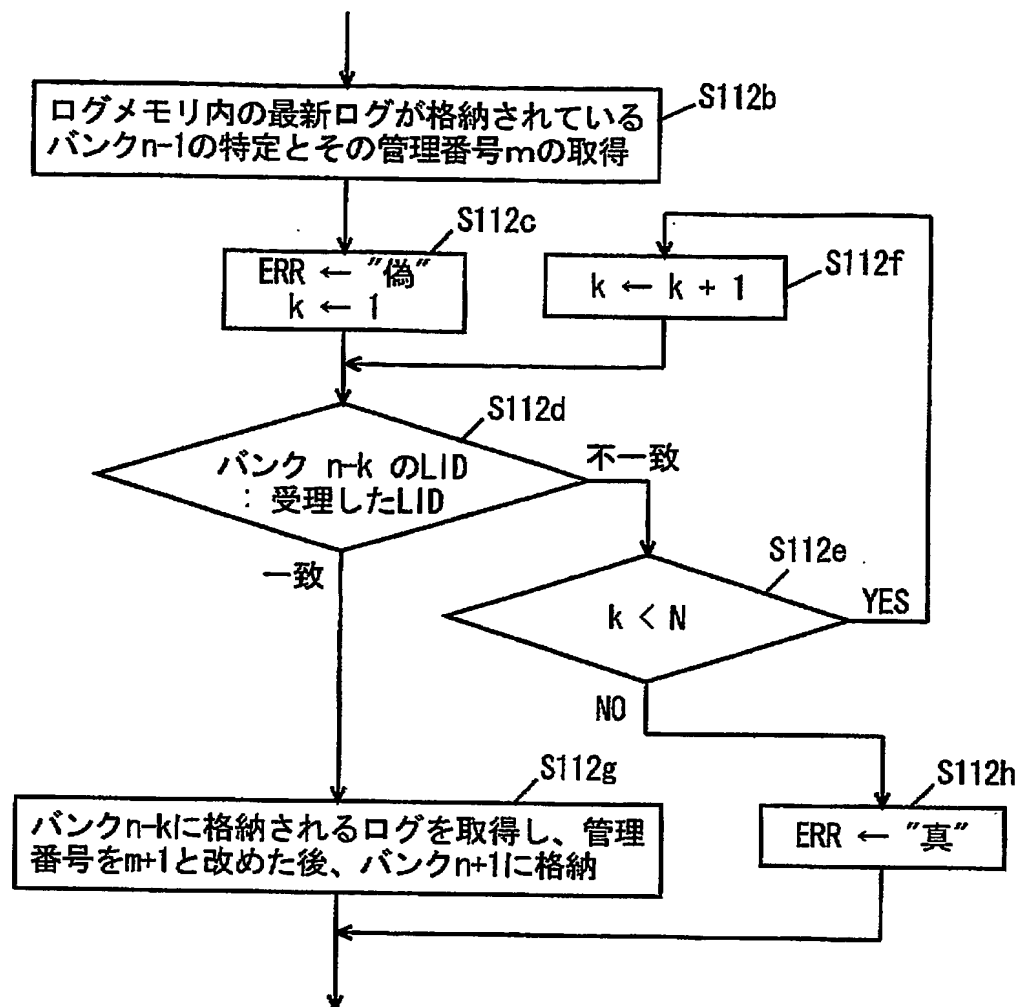
【図 14】



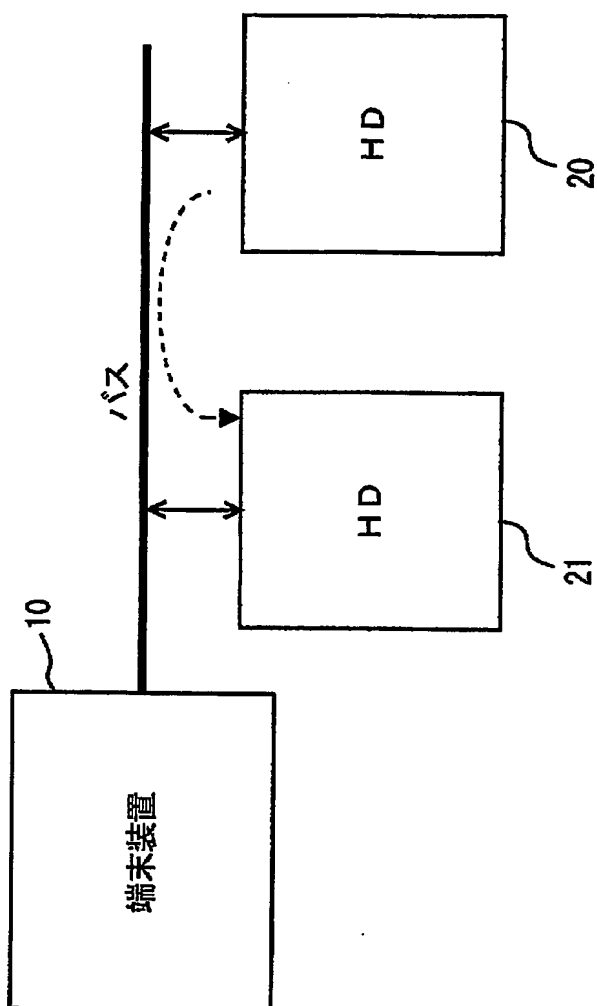
【図 15】



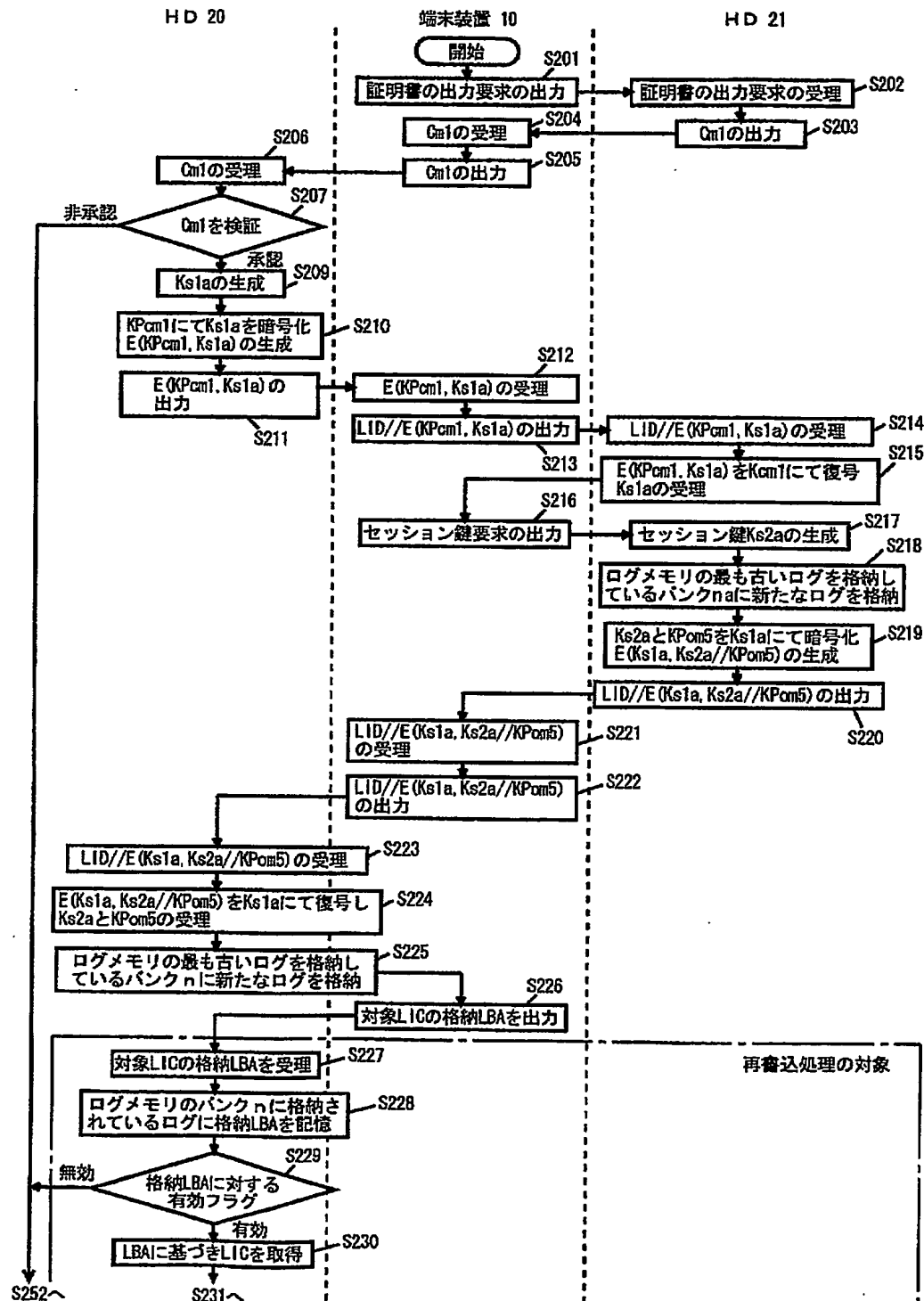
【図 16】



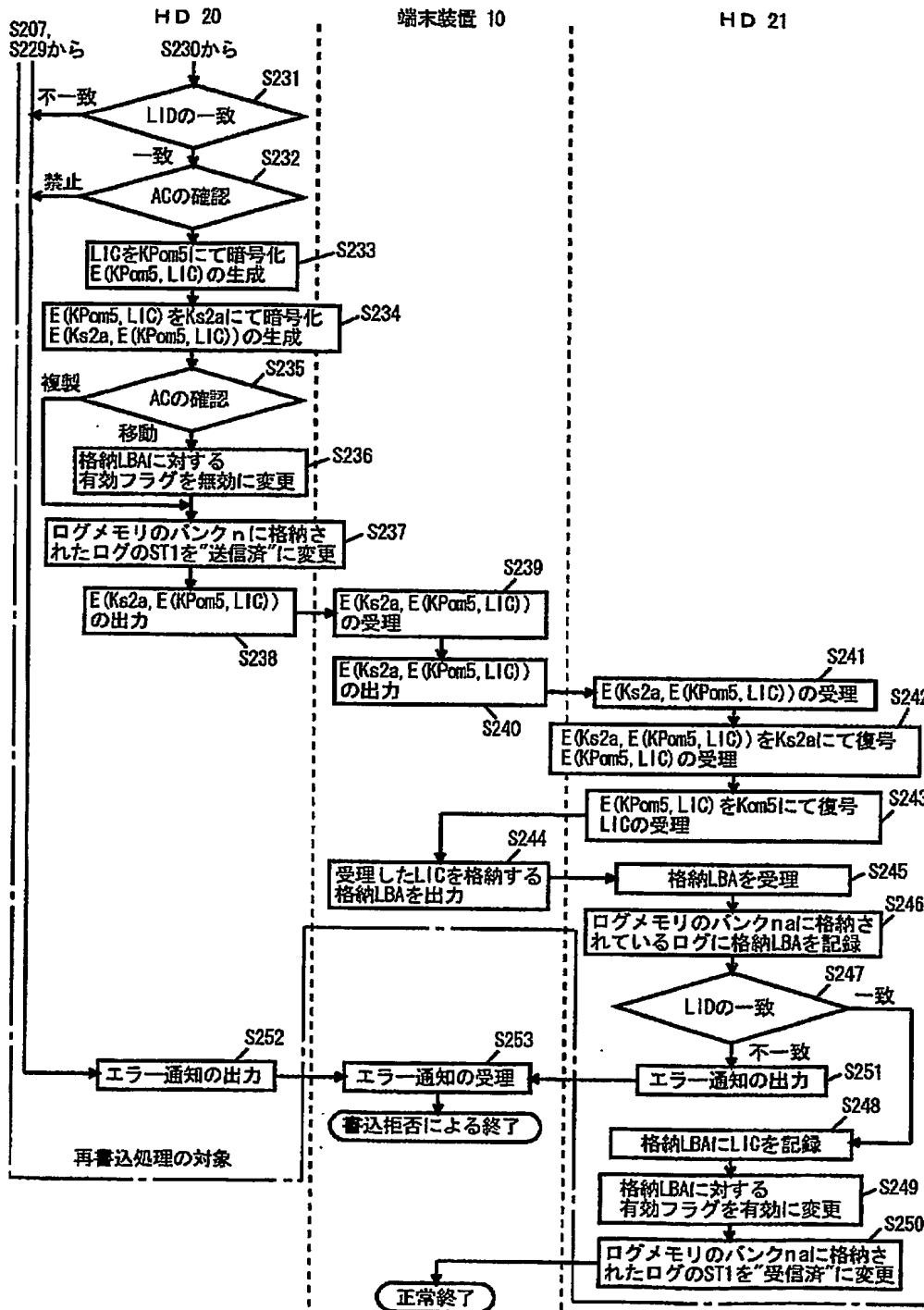
【図 17】



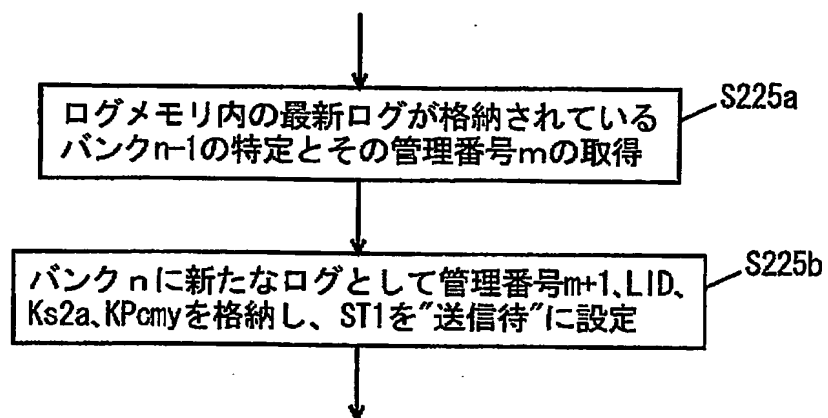
【図 18】



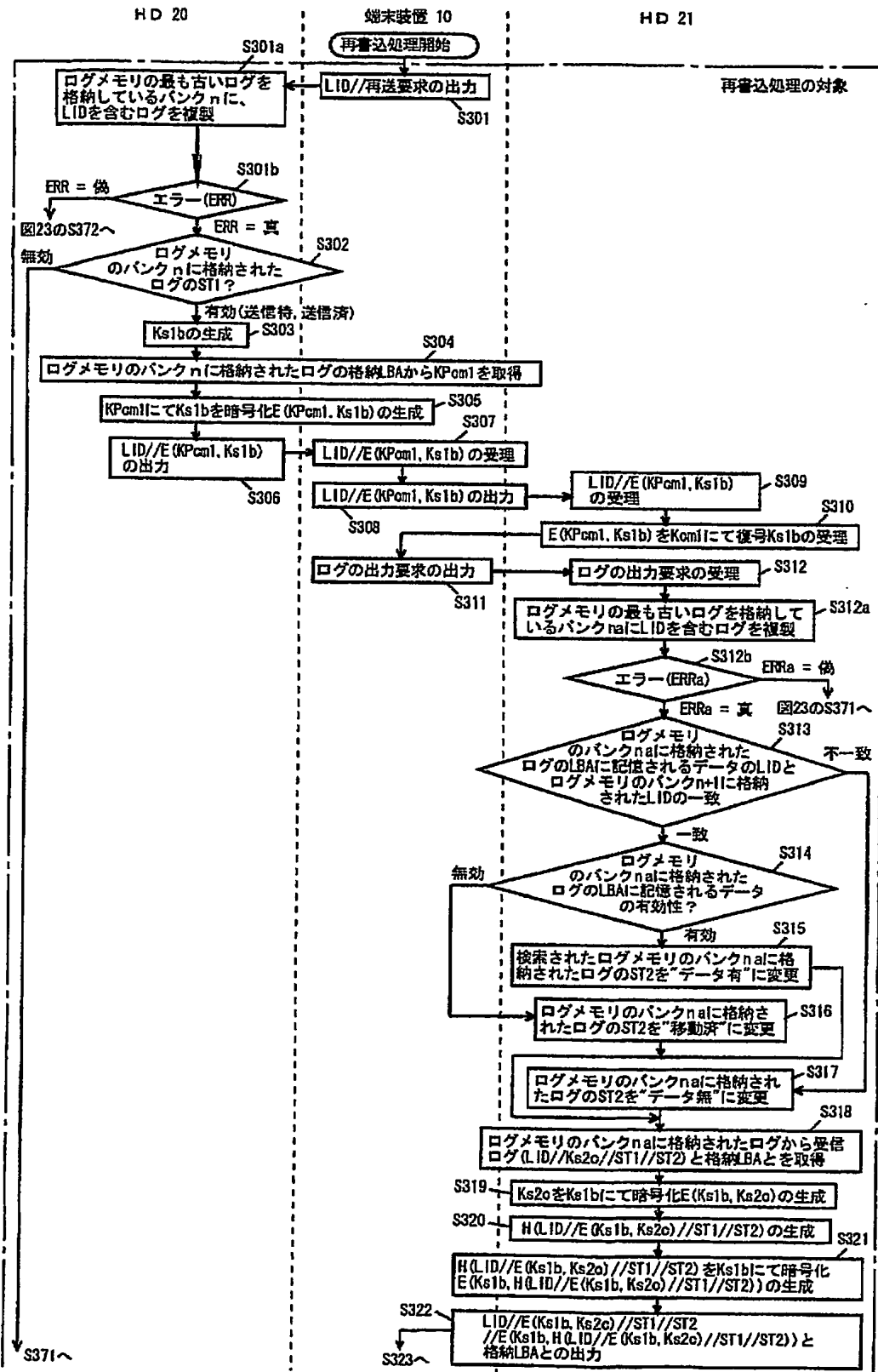
【図 19】



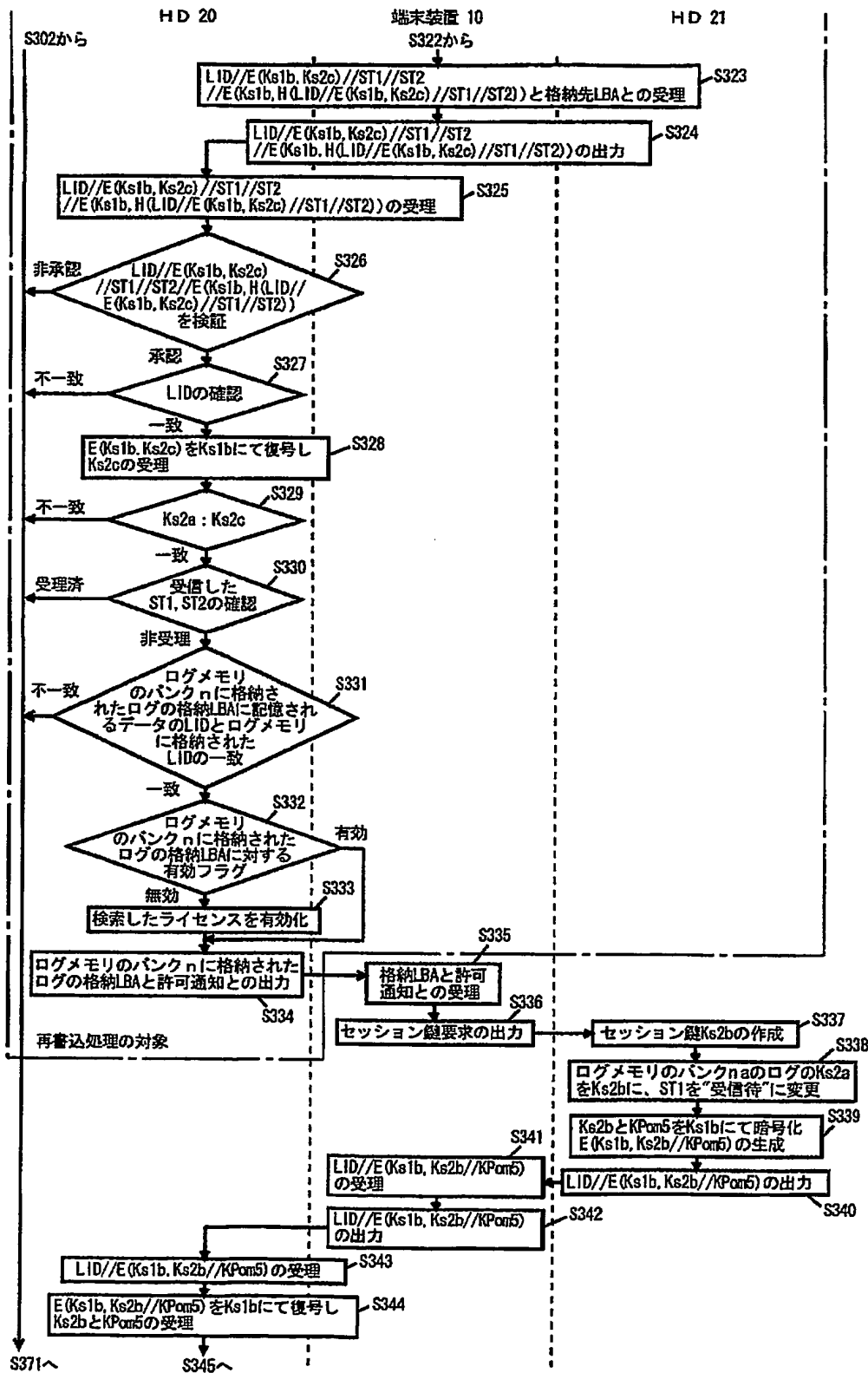
【図 20】



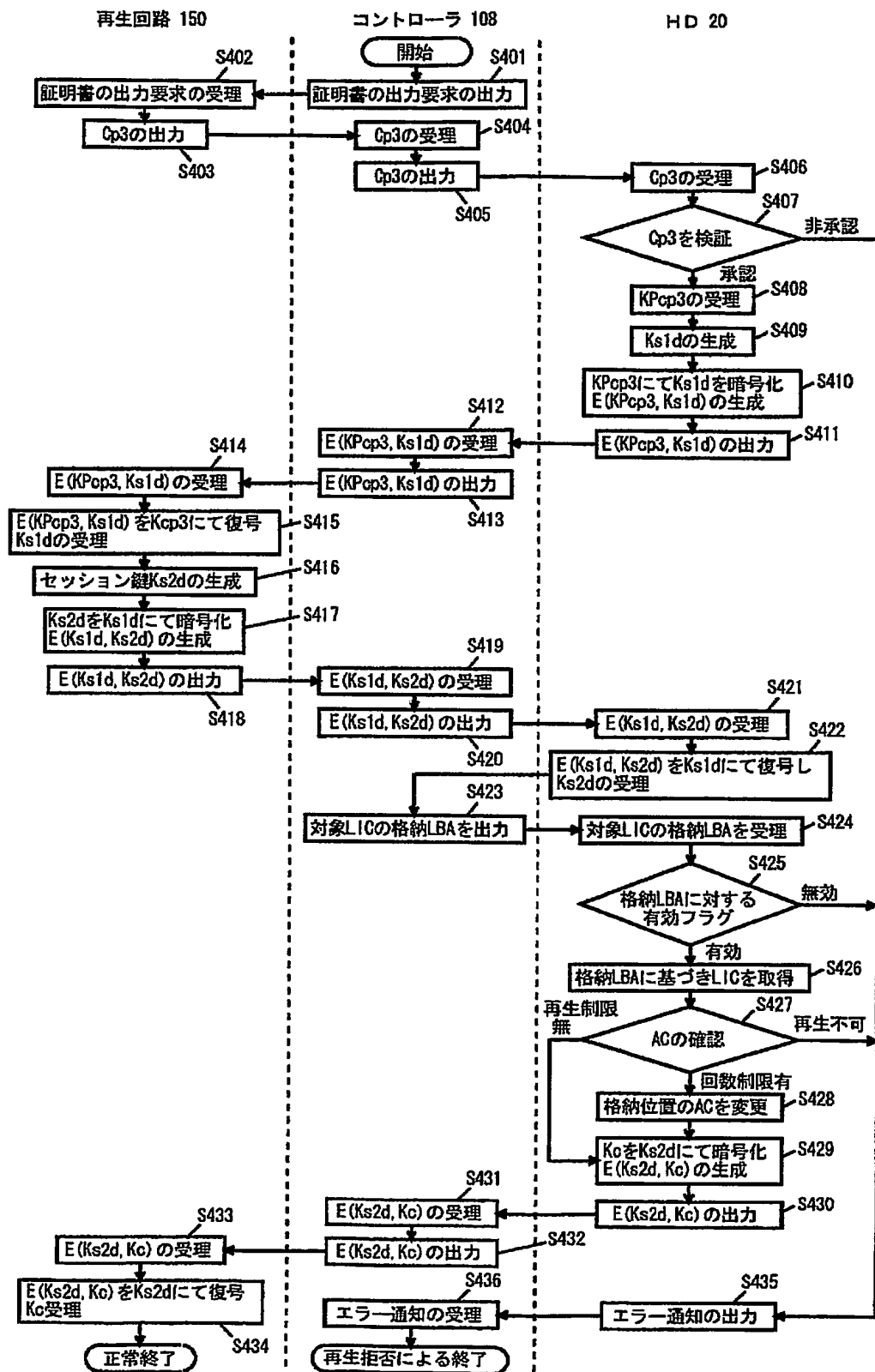
【図 21】



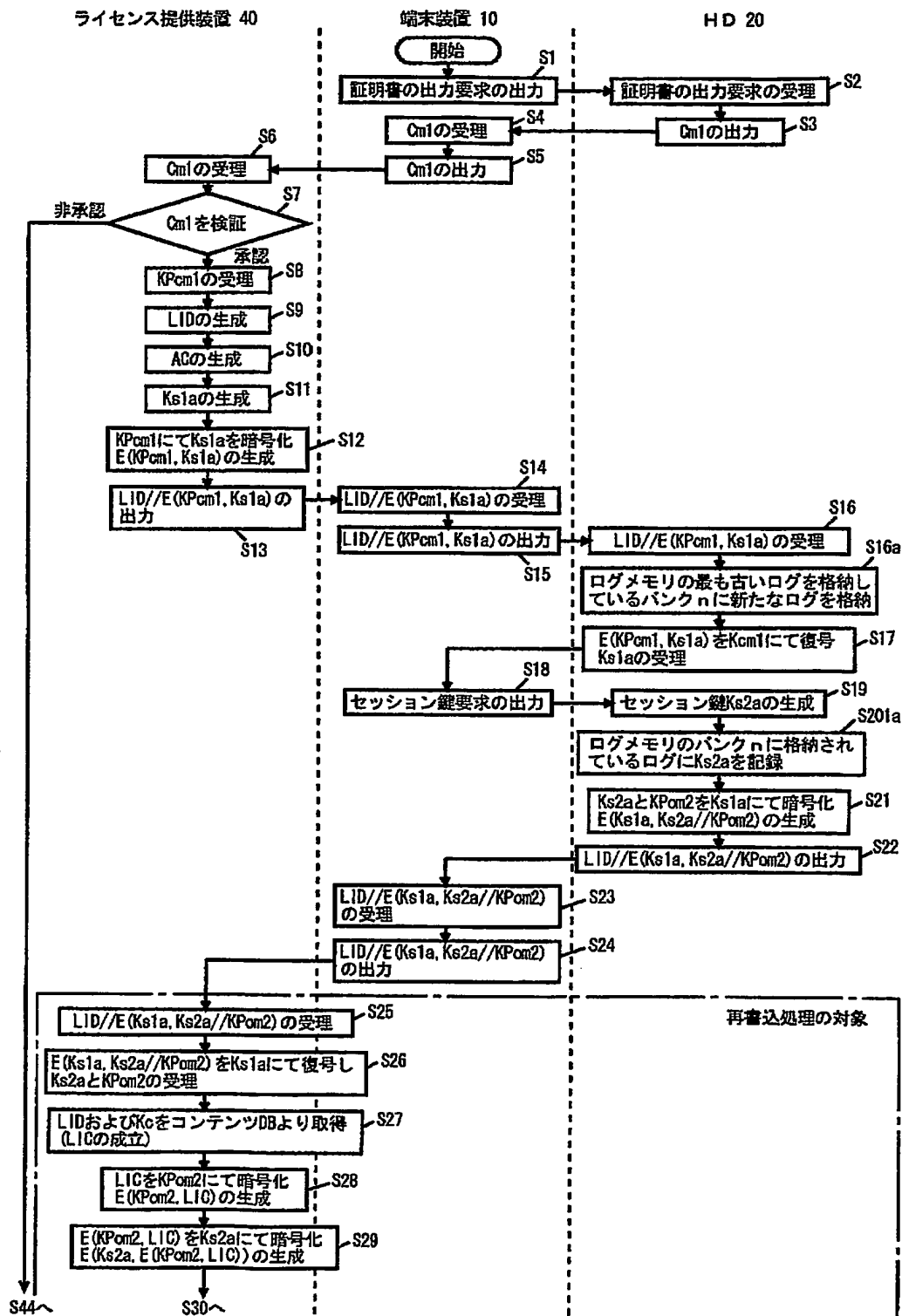
【図 22】



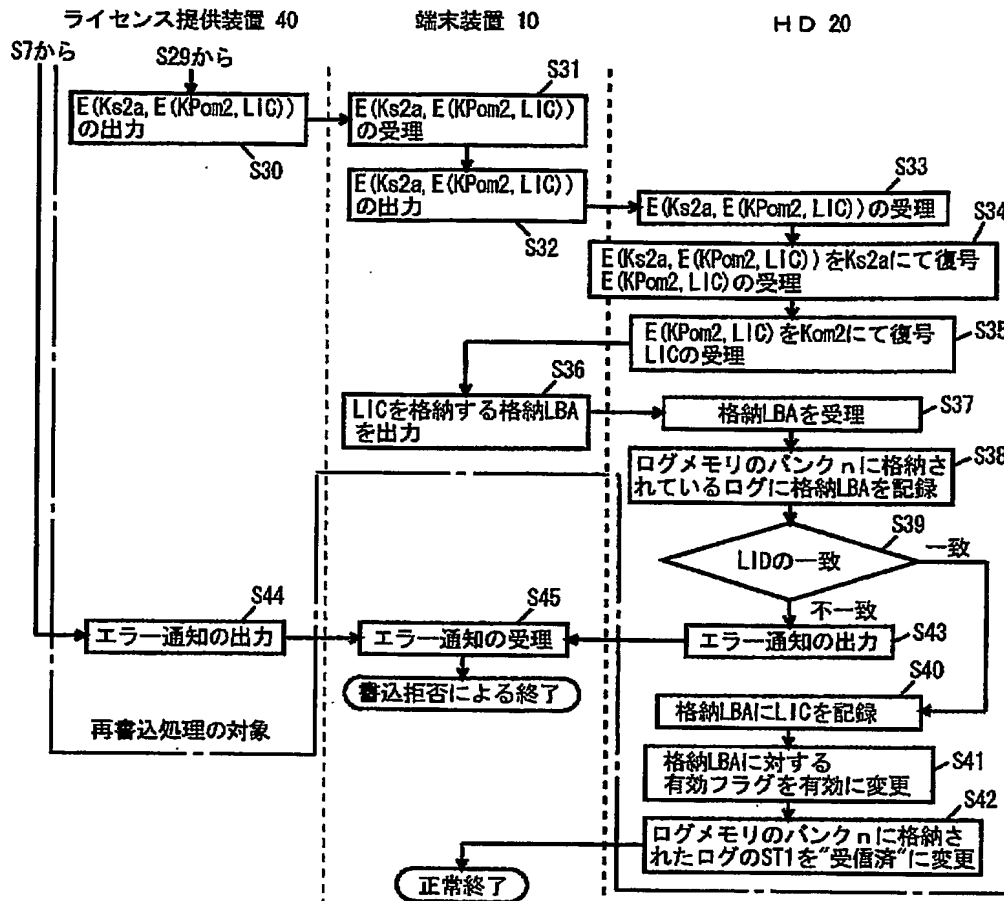
【図 24】



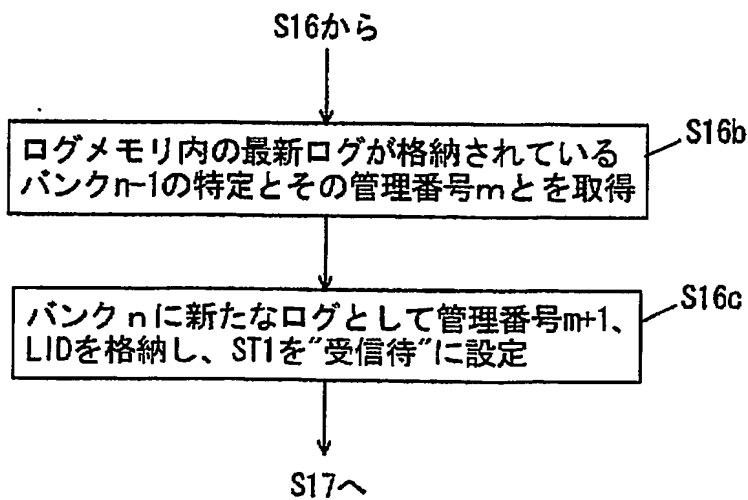
【図 25】



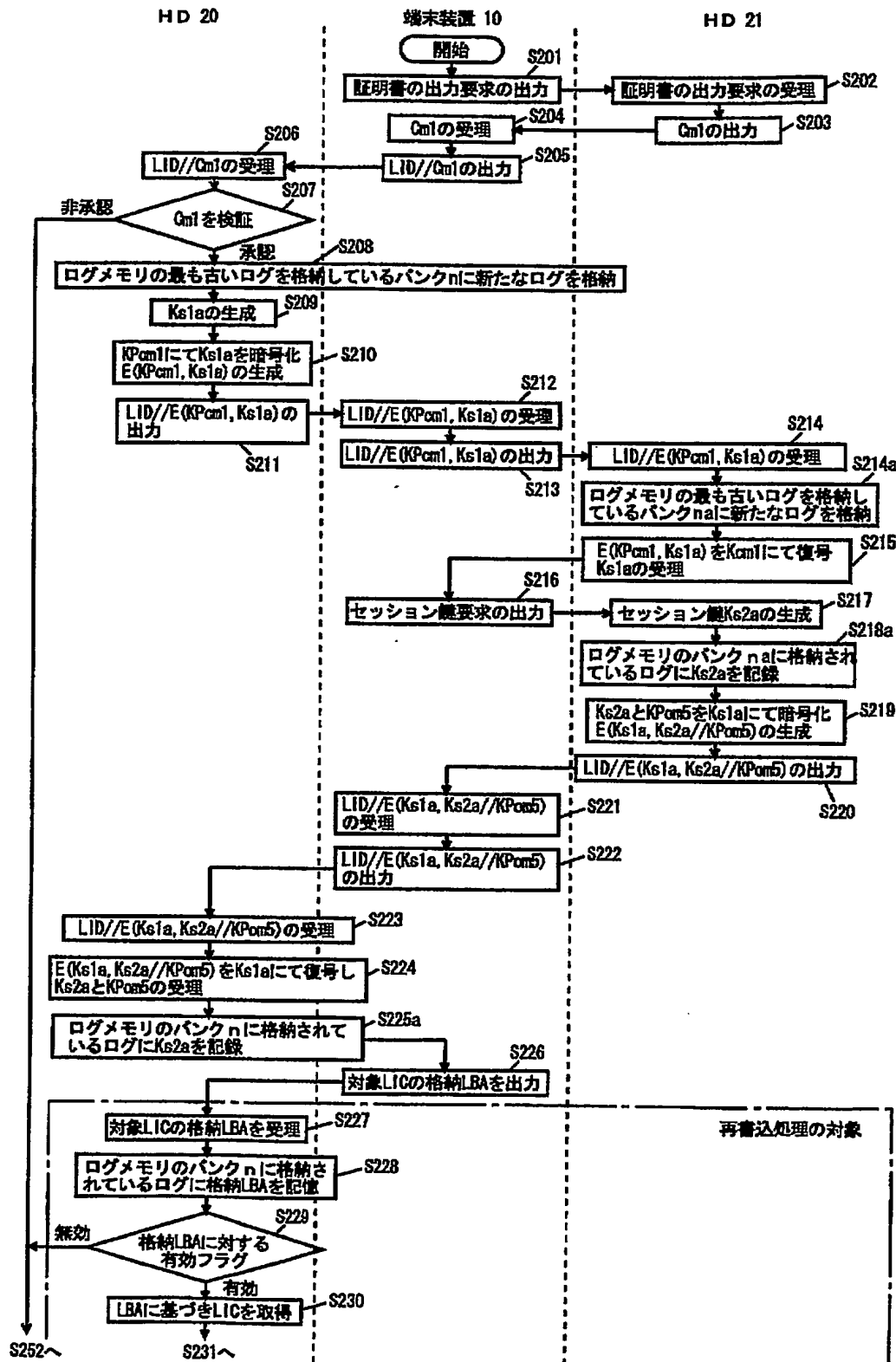
【図 26】



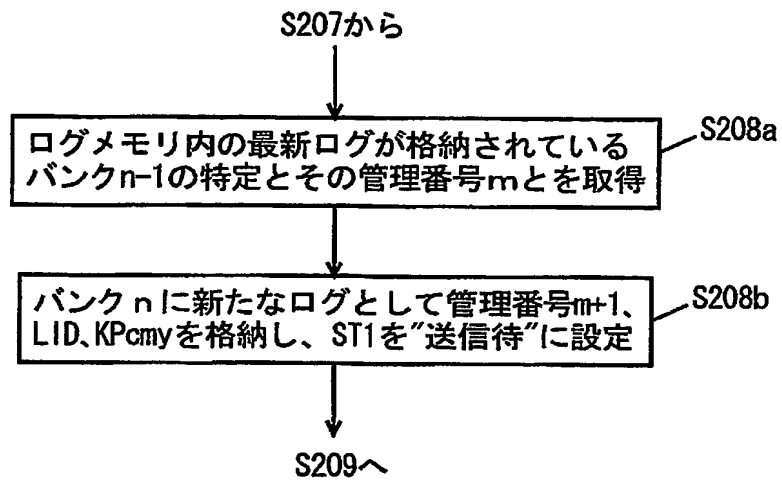
【図 27】



【図 28】



【図 30】



【書類名】 要約書

【要約】

【課題】 ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための複数の履歴情報を重複することなく格納できるデータ記憶装置を提供する。

【解決手段】 データ記憶装置は、ログメモリ 253 を含むセキュアデータ記憶部 250 を備える。ログメモリ 253 は、複数のバンク 2531～253N から成り、複数のバンク 2531～253N にリング状に履歴情報を格納する。複数のバンク 2531～253N の各々は、アドレス 0～N-1 によって指定される。バンク 2531～253N の各々に格納される履歴情報は、管理番号領域 2541 と、ライセンス ID (LID) 領域 2542 と、Ks 2x 領域 2543 と、ST1 領域 2544 と、ST2 領域 2545 と、KPcm y 領域 2546 と、LBA 領域 2547 とを含む。

【選択図】 図 7

特願 2002-216750

出願人履歴情報

識別番号

[000001889]

1. 変更年月日

1990年 8月24日

[変更理由]

新規登録

住 所

大阪府守口市京阪本通2丁目18番地

氏 名

三洋電機株式会社

2. 変更年月日

1993年10月20日

[変更理由]

住所変更

住 所

大阪府守口市京阪本通2丁目5番5号

氏 名

三洋電機株式会社

特願 2002-216750

出願人履歴情報

識別番号

[000005016]

1. 変更年月日

1990年 8月31日

[変更理由]

新規登録

住 所

東京都目黒区目黒1丁目4番1号

氏 名

パイオニア株式会社

特願 2002-216750

出願人履歴情報

識別番号

[000005108]

1. 変更年月日

1990年 8月31日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台4丁目6番地

氏 名

株式会社日立製作所

特願 2002-216750

出 願 人 履 歴 情 報

識別番号

[300017636]

1. 変更年月日 2002年 4月 4日
 [変更理由] 住所変更
 住 所 東京都千代田区丸の内1-3-1 東京銀行協会ビル14F
 氏 名 フェニックステクノロジーズ株式会社

2. 変更年月日 2002年 8月16日
 [変更理由] 住所変更
 住 所 東京都新宿区新宿4-2-18 新宿光風ビル6F
 氏 名 フェニックステクノロジーズ株式会社

3. 変更年月日 2003年 1月 8日
 [変更理由] 住所変更
 住 所 東京都千代田区丸の内1-3-1 東京銀行協会ビル14F
 氏 名 フェニックステクノロジーズ株式会社

特願 2002-216750

出 願 人 履 歴 情 報

識別番号

[000005223]

1. 変更年月日

1990年 8月24日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中1015番地

氏 名

富士通株式会社

2. 変更年月日

1996年 3月26日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中4丁目1番1号

氏 名

富士通株式会社